Stickybeak by proxy

November 28, 2012

Hayden Glass (hglass@srgexpert.com, +64 21 689 176)

Stickybeak by proxy (Part 1)

Our ideas about privacy need redefining in the internet age

I consider myself a fairly typical internet user. Google for web search, a Gmail account for email, calendar and contacts, the Chrome browser for surfing, and my Google drive for a whole host of documents stored and shared in the cloud. On my Android phone I have 60 or so apps installed. I have no Facebook account, but I am on Twitter. I use Dropbox to share files, Flickr for my photos, iTunes for music, and Tumblr and WordPress for blogs. Plus, like the rest of you, I use online banking, shop online, and get my news nearly exclusively from online sources. I provide my location to make Google maps work better and also to help get better search results, but I click "Deny" when my phone gives me the choice to share location with any particular website.

I am sharing, therefore, quite a lot of information on the internet. This is an entirely standard way of life. Around 80% of us use the internet, and 80% of users report using Facebook.

The internet is such a part of daily life that we now share information unconsciously. Everything we do online creates a record and we don't think too much about what happens to it. In US academic Daniel Solove's vivid phrase, "data is the perspiration of the Information Age". Others, like American computer security specialist Bruce Schneier, think of your click-stream as a type of pollution, in the sense that it is created by doing some useful online task but it can have unpleasant side-effects that need to be managed.

In Part 1 of this post we take a brief look at the online privacy environment and what makes it different. In Part 2 we look at how laws are changing to adapt to it.

Something new under the sun

Problems of information privacy are much more difficult in the internet age because the internet itself is so widely available, and information flows on it are difficult to control.

The internet has no borders, and is not based in any particular country. The location of service providers or users is generally unimportant: information available in one place is available in all, and it is difficult to control or trace the flow of data. Content is continually being added or modified, but content is also persistent, i.e., information that was once on a website can be searched for and retrieved even after the content of the site has changed.

The internet is also tricky for governments to control. There are, of course, still telecommunications operators who connect you to the internet. They have extensive physical investments, powerful brands and reputations to uphold. But service providers who hold information about you are generally not dependent on individual governments for resources at all. Most of the New Zealand internet's most popular services are provided by US firms based in California with servers all over the world, and with little local presence here. The ability of the New Zealand government to influence the

activities of, say, Facebook is limited, and given the aterritoriality of the internet, it is often not clear how firms can navigate the thicket of different national responsibilities.

Privacy, of course, is also a non-internet problem. Those holding information need to not, for example, lose sensitive government data in the internal post, or leave their computer systems open for members of the public to access.
But often internet users do not realise how much they are sharing (see these unfortunate Belgians), or what the consequences are. Facebook stands accused of deliberately making it hard for users to control their own privacy, and even the most sophisticated can get it wrong, releasing data that they think is innocuous (like AOL or Netflix that turns out not to be when combined with other public data. See also a local example.

Gold in them thar hills

The major online services companies have also raised substantial privacy concerns by mis-estimating what their users are happy with: cue dismay when Mark Zuckerberg, Facebook CEO, said that his firm was built on privacy expectations that all users might not share and the furore over changes to Facebook's privacy settings that have led to EU and FTC regulatory intervention, or when Google's then CEO Eric Schmidt said that if you want to keep something private online "maybe you shouldn't be doing it in the first place".

With all of this information about your online activities able to be discovered, there is money to be made in sifting through it, tying it together, and then selling the profiles to online advertisers.

Consider Rapleaf, a US outfit that matches email addresses with a range of public data including Zip code, age, income, property value, marital status and whether the person who controls this email address has children. It claims to have data on over 80% of US email addresses, and charges 0.5 cents per match.

Or this article (registration required), a deal between Facebook and a firm called Datalogix that allows the site to track whether ads seen on Facebook lead users to buy those products in stores. Datalogix buys consumer loyalty data from retailers, and matches email addresses in its database to email accounts used to set up Facebook profiles.

Generalised concern

It is hardly surprising that people are concerned about online privacy. Americans say their biggest perceived privacy threat is social networking services like Facebook and Twitter (they are also worried about unmanned drones, electronic banking, GPS/smartphone tracking and roadside cameras).

New Zealanders are worried too. A Law Commission survey revealed that 84% of respondents were concerned about "the security of personal details on the internet", more than were concerned about "confidentiality of medical records" (78%) or "government interception of telephone calls or email" (72%).

Expectations of privacy clearly depend a lot on context. Information I share with my mother I may not wish to share with my friends (sorry guys), and information I share with my friends I may wish to keep secret from a potential employer. Information that I directly and intentionally share (e.g., via Twitter) is less sensitive than information that I do not know is being collected. I would consider my browser history, my email and my search history more sensitive than my purchase history from Amazon.com. I am pretty

relaxed if information about these things is used just to target online advertising. I am less relaxed if these data were put together and used to establish my identity or calculate my credibility and trustworthiness.

And since my list of privacy preferences will not be the same as yours, it becomes clear that the question of online privacy is about the limits of my ability to control the flow of information about me, and my basic point here is that the internet age means that I have less control than before.

If users are concerned about control but feel (and to some extent are) powerless, what help does the law provide? We take up that story in Part 2.

Stickybeak by proxy (Part 2)

In Part 1 we looked at some aspects of online privacy. In this article we look at the law.

Can the old dog still hunt

New Zealand's privacy laws are generally considered to be pretty sound. The Privacy Act began life in 1993 describing a set of principles and giving you a bunch of rights in relation to controlling the collection, use and disclosure of personal information.

"Personal information" is defined in the Act as "information about an identifiable individual", i.e., information from which you can be identified. If an agency is collecting anonymous information about your movements online, that is one thing, but if your online profile grows to the point that you could be identified from it, the rules in the Privacy Act can apply. As discussed in part 1, the line between anonymous and identifiable can be pretty uncertain.

The Law Commission looked at the Act in a three-year review of privacy laws that was completed in August 2011. It continues to believe that self-protection is the best protection, but suggests a substantial set of changes aimed at improving the law including:

- new powers for the Privacy Commissioner to act against breaches of the Act without necessarily having received a complaint, and allowing it to order those holding information to comply with the Act or submit to an audit of their privacy rules, and
- measures to minimise the risk of misuse of unique identifiers, and require those holding information to notify you if your information is lost or hacked, and
- controls on sending information overseas.

The government agrees that it is time for substantial changes to the Act, although it does not agree with everything the Law Commission has proposed. A new draft Bill is expected next year.

To the ends of the earth

One obvious issue in the internet age is the lack of matchup between the international nature of internet services, and laws that are limited to the borders of any particular nation. A modestly-sized nation at the end of the world, like New Zealand, has limited ability to influence foreign organisations who may not have any local presence, although our Privacy Commissioner has taken action against reputable major players offering services in this country.

One answer is to harmonise our laws with other countries, or rely on the big fish to protect our privacy. If the US or the EU forces firms to improve privacy protections we will benefit. The US Federal Trade Commission can legitimately argue that its actions will protect users in other countries (see the summary of a talk from Nethui 2012 here, and it is focused on this stuff. Vivian Reding, then the EU Justice Commissioner said that privacy for European citizens "should apply independently of the area of the world in which their data is being processed …. Any company operating in the EU market or any online product that is targeted at EU consumers must comply with EU rules". The French data protection agency is investigating Google's new privacy policy.

Another evident challenge to existing privacy law is to the notion of "informed consent". As a legal principle it is fine, i.e., your favourite online service has a privacy policy and you consent either directly to it by checking the box and clicking "I accept" or implicitly by using their service. So long as the policy does not breach the law and the service follows their own policy, they are legally blameless.

In practice you likely haven't read the policy, and you may not be in a position to avoid surrendering some privacy in any case. Participating in society increasingly requires online interaction, and any online interaction will involve sharing some information. Legally operators can rely on your click to indicate consent to their privacy policy, but in practice you cannot really withhold it.

One solution could be crowd-sourced reviews of online privacy policies, or organisations that rate others policies. There are similar troubles with the terms of licensing agreements to which you have to consent in order to use software.

Fit for purpose

Users have options to protect themselves online if they care to. They can avoid being tracked, ensure their privacy settings for social media services are well considered, disable cookies, turn off javascript, use fake Gmail or Facebook accounts, use incognito modes on their browsers, access the online world through a VPN or a range of other things. The Privacy Commissioner has guidance also. And you either have now or will soon also have an option to turn on a "do not track" option in your browser, that will impede the ability of firms to piece together your internet history as you find your own trail through the online garden.

Sadly users mostly do not avail themselves of these options. That may be because some impede the internet experience a bit. Or because users do not care to change their behaviour much despite saying they are worried about online privacy.

In these circumstances, there will continue to be debate about how far users can or should take responsibility for their own protection, and how far the law needs to go. This battle is the natural result of the standard model for internet services, i.e., if you want free internet services, you need to realise that your eyeballs are the price. No one should be surprised that advertisers try to make their services more effective by learning more about the brains behind those eyeballs.

Hayden Glass is a Principal with the Sapere Research Group, one of Australasia's largest expert consulting firms. Thanks to Rick Shera (@lawgeeknz) for instructive conversation.

This article was originally published on the TUANZ blog.