Are access and correction tools, opt-out buttons, and privacy dashboards the right solutions to consumer data privacy?

Akiva Miller

Consumer data access and correction

In September 2013, date broker Acxiom announced the launch of a new website, Aboutthedata.com, which allows individuals to view and correct information that Acxiom collects about them, as well as opt out of inclusion in its products for advertisers. The new website marks a first attempt by a large consumer data broker to allow consumers some tools to view and correct data about themselves. Other data brokers have not yet followed suit.

In a recent panel, FTC Commissioner Julie Brill commended Acxiom's move, but nonetheless said that data brokers should do more to give consumers better knowledge and control over their data. But the site has major shortcoming. It does not show consumers all the information collected about them, the information is often riddled with errors, and consumers may only opt out of Acxiom's advertising products, but not out of those used for employee screening and fraud detection. Stories of Acxiom's poor data quality was also noted here, and here.

Meanwhile, in recent months, Julie Brill announced her own initiative - "reclaim your name". The initiative will encourage data brokers to voluntarily adopt an industry standard and join an online platform for giving consumers access to data collected about them, allow them to opt out, and give them the opportunity to correct information about themselves. Details remain sketchy, for now.

Of course, Google has for a while now allowed users to view and alter the demographic data and interests inferred from users' search history, their clicks on advertisements, and their YouTube viewing records, as well as opt-out of targeted ads. Like Acxiom's inferences, these too are frequently far off the mark.

Opting-Out of data aggregators

A number of data brokers besides Google and Acxiom (such as BlueKai and Rapleaf) allow individuals to opt-out of their advertising products. None of the data brokers offer consumers, as yet, the choice not to have information gathering about them collected altogether. In fairness, doing so would be difficult for brokers, since they typically acquire large databases of information for a wide array of sources, and only rarely interact with data subjects directly.

But that is changing, at least a little.

Recently, the Digital Advertising Alliance (and its European affiliate, the European Interactive Digital Advertising Alliance (EDAA)), launched Ad Choices and YourOnlineChoice.com), which allow users to opt out of ad networks' and data brokers' tracking cookies. The self-regulatory initiative also includes a code of conduct, an information website for consumers about industry practices, and a little icon on banner ads to signal their participation in the initiative.

Unfortunately, the "opt-out" option in these websites presents users with the paradoxical choice of having to change their browser settings to accept a special “opt-out cookie”, even if they usually block third party advertiser cookies. (EU users can also install the “protect my choices” browser extension to solve this problem). Bewildered uses find themselves in a situation where two privacy-enhancing technologies are at odds with each other, and they are left guessing which will protect their privacy better. For now, the Ad Choices website is running in Beta and is still buggy.

Meanwhile, all this attention to tracking cookies may soon become obsolete, as Google, Microsoft, and Facebook prepare to employ new technologies to track users that bypass cookies altogether, and track users directly through the identifying numbers in their devices.

Dashboards

Privacy dashboards, those consolidated lists of privacy options, have been touted as the “right” approach to privacy control (see, e.g. support for privacy dashboards by the FTC and World Economic Forum, to name a few).

But do privacy dashboards always make controlling privacy easier?

Google’s privacy dashboard and other privacy tools allow users to access information collected about them (their account activity and web and YouTube viewing history) and to control many privacy settings. But these options are only available to users who sign in under their Google+ account. At the same time, Google’s privacy policy makes clear that it also collects information on users who do not sign in under a Google+ account. Thus, users again face a paradoxical choice: Sign in to Google’s services and use them in an identified manner, and you are allowed to control your privacy settings. Choose to be anonymous, and you will still be tracked but given no privacy options at all.

Or consider Facebook’s recent privacy decisions. In the past year, Facebook took away the option not to be searchable by name. What’s more, since Facebook’s Graph Search was rolled out in January, it became possible to find users in ever more sophisticated ways rather than by name alone. It is now much more complicated to maintain one’s privacy on Facebook. Although users can still control what content others can see, asserting one’s privacy requires many more specific settings for specific kinds of content, and can no longer be achieved with a single privacy option.

Does having more control tools mean better privacy?

Allowing consumers a chance to access and correct information collected for marketing purposes will test the claims that consumers actually desire more relevant and personal advertising and become less nervous and more accespting of tracking when they are able to see the information and understand how it is used. This narrative comports well with the FIPPs model of privacy, which associates privacy with individual choice and autonomy, and fits in with the modern mantra that privacy policy should regulate data uses, not data collection.

But critics may chuckle at the suggestions that consumers will benefit from correcting data brokers’ misinformed guesses about them. As some suggest, the entire endeavor is simply a stunt to deflect criticism of the consumer data industry over its unfettered gathering of data by shifting the burden of privacy protection on to the shoulders of consumers themselves.

Whichever the case, the access and correction trend departs from the "opt-out" view of privacy, which castes privacy as entirely antagonistic to consumer targeting. "Opt-out" is inherently contradictory. On the one hand, consumer data brokers have long argued that aggregated consumer data is the key to giving consumers what they really want – more relevant ads (and the free stuff it pays for). At the same time, they acknowledge that users deserve a right to privacy, which they interpret as opting-out of targeted advertising databases. The result: data brokers begrudgingly give users the opportunity to opt-out, but hope they will not exercise this choice.

What's more, companies that offer an "opt-out" option (like its cousin, the "unsubscribe" option in some spam messages), and privacy dashboards insist on retaining the power to control the means and the terms of the opt-out. Thus, paradoxically or not, the provision of opt-out options and dashboards goes hand in hand with the development of ever more powerful gathering abilities that circumvent or make obsolete privacy-enhancing options built into internet browsers, or added on to them.

But here we may pause and wonder – what would a truly privacy-respecting advertising industry look like?

Some interesting initiatives

If the state of consumer access and control to data appears unsatisfactory, there are a few interesting initiatives that are thinking of new digital applications that will put more control in the hands of individuals over the data they share with businesses (thanks to Doc Searls for these references):

Vendor Relations Management (VRM): The idea is to give users digital tools to communicate and maintain their own relationships with the businesses, without being dependent on the marketing and Consumer Relations Management (CRM) platforms of those businesses.

The UK's MiData initiative aims to give users better access and tools to understand the data gathered on their use habits by phone, electrical, bank accounts, and credit cards. The motivation is not so much to protect privacy as it is to empower consumers and help them make better choices.

MesInfos – A French initiative, whereby 300 participants are allowing application developers to access personal information gathered about them by a number of key partner organizations (a bank, mobile provider, Google, the post bank, and insurance company, a retailer, etc.) over a six-month period. The developers will then build innovative applications and services around this data for consumers' own use, while researchers study the impact of the new applications on the habits and opinions of the participants.

Any thoughts? Know of any other privacy tools or consumer transparency tools? Please Let add to the conversation.