Online Privacy: How to Control Your Personal Data

Most people don't think of the phone book as that yellow block of razor-thin sheets anymore. It's been digitized, along with your contact information, habits, and interests. In fact, all the stuff that used to be offline — like government records, court records, product registrations, and subscriptions — has moved to the web. And we're adding new types of information all the time. According to "Zuckerberg's Law," [1] people share twice as much information as they did the year before. The result: A feeding frenzy has emerged for personal data.There are two types of companies profiting from all the personal information online. Companies whose privacy policies you don't read, and companies you've never interacted with. In the first camp are companies like OnStar, which can sell your car's GPS data [2], Verizon which sells your location and browsing history [3], and the many U.S. states that sell [4] their residents' DMV records.Then there are the data brokers, who compile detailed profiles about you from as many sources as they can. Data brokers sell these profiles to anyone who will pay, whether they're a marketer or a creepy ex. And the problem is getting worse. Since 2005, the number of data brokers has more than doubled. That's because it's becoming easier to scrape, steal, and package your data. When our telephone privacy was invaded by telemarketers, we got the Do Not Call list. When it became apparent that our online and offline privacy was being invaded by new business models, we got the proposed Privacy Bill of Rights. Unfortunately, technological innovation radically outpaces the ability of government to regulate it, and the Privacy Bill of Rights gives a free pass to data brokers and third parties to buy and sell your personal information. That leaves protecting your privacy in your hands. Here's how to get started.

1. Cut Off Data Brokers

Data brokers are a self-regulated industry, which means they control how you can remove your information from their databases. Some require you to fax an opt-out

request. Others require you to fill out a form on the web, and some require snail mail. Certain data brokers will even ask you to confirm or follow up via email. Others will say you must send in proof of identification, like a State ID. This process is complicated by design.The Privacy Rights Clearinghouse maintains a list of data brokers [5], and a link to their privacy policies or opt-out pages. But this list includes 147 companies. Fortunately, most of the companies listed are small, get no traffic, and are a poor outlet for your data. You're going to first want to target the big boys which include Acxiom, BeenVerified, MyLife, Intelius, Spokeo, Rapleaf, White Pages, and PeopleSmart.

2. Ensure Data Sources Are Controlled

The two primary sources of your data are government records and social networks. There's not much you can do about public records, besides getting old criminal records expunged, purchasing real estate using an LLC [6], and avoiding divorce.Social networks, however, are totally in your control and should never be a source of data leakage. Everything that you consider private (contact information, family, pictures, interests…) can become public if you're not careful. For starters, restrict your privacy settings to the most protective possible, such as allowing only your direct friends and connections to see anything at all. Basic information, such as your name, city, and headshot can remain public, but anything beyond this should be off limits. Also:

- Don't accept requests from people you don't actually know. Bots masquerade as people now.
- Don't use social logins — Facebook, Twitter — to log on to websites or apps if an email alternative exists. If a website seems suspicious and they only allow social logins, forget it.
- When your friends use social apps, said apps can access your information. This is a massive vulnerability. Restrict this access by going to Privacy Settings -> Apps, Games, Websites -> How people bring your info to apps they use. Make the proper adjustments here.

3. Contact Elected Officials

Lastly, your health records are totally off limits, your personal, financial, and social information should be, too. Tell Congress [7] that the Privacy Bill of Rights should include restrictions on how data brokers can transmit and sell your personal information, and file a complaint [8] with the FTC against the deceptive practices of data brokers when they complicate the opt-out process.Remember, privacy is your decision. Fight for it.

www.mashable.com [9]

Posted by Janine E. Mooney, Editor

May 22, 2012

Links:
[1] http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CFUQFjAA&url=http%3A%2F%2Fbits.blogs.nytimes.com%2F2008%2F11%2F06%2Fzuckerbergs-law-of-information-sharing%2F&ei=Liu6T-2SFoHC6AGM0_TJCg&usg=AFQjCNHcFSitEl0fCZTBj9_lxCyOw0Dy6Q
[2] http://www.wired.com/threatlevel/2011/09/onstar-tracks-you/
[3] http://money.cnn.com/2011/11/01/technology/verizon_att_sprint_tmobile_privacy/index.htm
[4] http://www.cleveland.com/open/index.ssf/2010/07/ohio_collects_millions_selling.html
[5] http://www.privacyrights.org/online-information-brokers-list
[6] http://mashable.com/2011/11/28/llc-corp-mistakes/
[7] http://www.usa.gov/Contact/Elected.shtml
[8] https://www.ftccomplaintassistant.gov/FTC_Wizard.aspx?Lang=en
[9] http://www.mashable.com