Testimony
of
JOHN M. SIMPSON
Consumer Advocate
with
CONSUMER WATCHDOG

Before the
Subcommittee on Information Policy, Census and National Archives of the House Committee on Oversight and Government Reform

On "Government 2.0, Part I: How Federal Agencies use Social Media and Other Web 2.0 Technology"

July 22, 2010

WEB 2.0: POWERFUL TECHNIQUES THAT DEMAND CLOSE SCRUTINY

Thank you Chairman Clay, Ranking Member McHenry and members of the committee for inviting me to participate in this hearing. I appreciate the opportunity to offer my testimony for your consideration. My name is John M. Simpson and I am a consumer advocate with the public interest group, Consumer Watchdog. Thank you for considering my testimony.

Established in 1985, Consumer Watchdog is a nationally recognized non-partisan, non-profit organization representing the interests of taxpayers and consumers. Our mission is to provide an effective voice for the public interest. Consumer Watchdog's programs include health care reform, oversight of insurance rates, energy policy, protecting civil justice, corporate reform, and political accountability. Over the past two years our Google Privacy and Accountability Project, funded partly by The Rose Foundation, a charitable nonprofit organization, has sought to safeguard consumers' online privacy by focusing attention on the practices of the Internet giant, Google. By holding Google accountable for its actions and encouraging the company to adopt necessary consumer privacy safeguards we believe we will help move the online entire industry in the right direction. You may read more about our project at our Website, http://insidegoogle.com.

I first became aware of the power of Web 2.0 techniques – such as social networking, blogging and online user-generated video – when I spent my vacation in 2008 to volunteer for the Obama Campaign in Joplin, Mo. Considering the successful use of the Web in that campaign, it is not at all surprising the administration has brought those methods and other cutting-edge technologies to be used in government.

There is no doubt in my mind whatsoever that these techniques can enhance citizens' participation in the democratic process and enhance both governmental transparency and responsiveness. Because many Web 2.0 techniques are widely embraced by young people and used regularly in their daily lives, adopting Web 2.0 methods will encourage younger generations to take a more active role in our democracy. It is important to note that it is not only the Executive Branch that has adopted these powerful tools. This committee's own Website, for example, features a Google YouTube video and links to the Committee's Facebook page, Twitter account and Google YouTube Channel. Perhaps all of the committee members are not fluent in Web 2.0 techniques, but clearly you have staff members who are.

But even though the federal government has rapidly adopted Web 2.0 because of its many obvious benefits, there are substantial concerns that must be addressed. All too often new technologies are adopted because of convenient benefits without adequate attention being paid to the potential harmful effects of the innovations. Technology is frequently implemented before necessary rules and regulations to protect society from negative impacts are written, let alone enacted.

So it is with Web 2.0. Government agencies have eagerly embraced FaceBook, Google's YouTube, and the like. This widespread use by government agencies of these services with links from the agencies' homepages is about strongest endorsement possible of the services. Any doubts or concerns the average American might have about them is all too quickly put to rest by prominent links to the services from the White House Web page, the State Department Web page and, yes, even this committee's home page.

But many of the companies involved in Web 2.0 services pose a real threat to consumers' privacy. Their business models are based upon tracking consumers as they use the Internet, gathering as much information about them as possible and using the data to sell ads to a largely unsuspecting audience. While Web 2.0 techniques have made government more transparent and responsive, there has been little such impact on the Googles and Facebooks of the world. They remain closed black boxes when it comes to revealing their methods and algorithms.

Consumers are followed around the Web, information about their habits is stored and analyzed, all while the online companies hide their practices behind dense, incomprehensible "terms of service" and "privacy polices" that appear to have been written by lawyers paid by the word who received a special bonus for opacity.

Worse, as has been demonstrated by such gross intrusions into consumers' privacy as Google's introduction of its social networking service, "Buzz," which publicly revealed the frequent email correspondents of users, Google's "Wi-Spy" snooping on home WiFi networks in 30 countries and Facebook's recent unilateral changes in privacy settings, the companies don't live up to their own professed privacy policies.

Where I go on the Internet and what I do there is my business. Consumers should have the right to control their data. It certainly should not sit indefinitely in corporate servers maintained by the likes of Google, Microsoft and Yahoo. And, just as there is a no-call list for the telephone, there should be a don't-track-me list for the Internet.

Silicon Valley's business model is to constantly push the envelope, gathering as much consumer information as possible because in the computer engineer's mind more data is always better even if you don't know what you will use the data for. You don't ask permission, because you can always ask forgiveness. But, Consumers deserve better.

The online industry's self-serving attempts at self-regulation have not delivered the privacy protections consumers deserve and require. Assurances from the likes of Google that the company can be trusted to respect consumers' privacy because its corporate motto is "Don't be evil" have been shown by recent events such as the "Wi-Spy" debacle to be unwarranted.

So, this is the current situation and the heart of the dilemma: Web 2.0 techniques offer government agencies powerful ways to enhance transparency and responsiveness, while also encouraging citizen participation. But most services simply do not respect consumers' privacy. The situation is exacerbated by the implicit endorsement of Google's YouTube, Facebook and other Web 2.0 services when they are featured on government Websites. How, the consumer might well ask, can there be a problem when the White House or a Congressional committee uses the services?

So, what can be done to both reap the benefits of Web 2.0 and protect consumers?

First, agencies need to be more explicit about what happens when consumers visit official Websites. Sometimes, whether out of coziness with a provider or a lack of diligence by the agency the situation is not as clear as it should be.

Let's look at what happened with the White House Website. When first launched after President Obama's inauguration, it featured embedded Google YouTube videos. When a consumer passed a cursor over the video image a tracking cookie was sent from Google to his or her browser. After objections from the privacy community to this stealth tracking and the apparent favoritism showed to Google, the White House modified the site. YouTube no longer hosts the video and no tracking cookies are placed on a visitor's browser. Moreover, if the visitor clicks on the links to the White House Facebook Page, YouTube Channel or Twitter Page, a warning is displayed making it clear that the consumer is leaving the White House site. This is as it should be and the White House Website now appears to set a standard for candor about a visitor's experience on a Website. (As an aside, I'm sorry to note that this committee uses embedded Google YouTube video that delivers tracking cookies to unsuspecting consumers and displays no warnings that when the visitor clicks on links he or she leaves the site for Facebook, Google YouTube or Twitter pages.)

Second, Congress must enact privacy legislation that will guarantee consumers control over their data and ensure their privacy when using the Web 2.0 services. Such legislation is now under discussion in the House Energy and Commerce Committee's Subcommittee on Communications, Technology and the Internet. A coalition of 11 consumer and privacy groups recently said the legislation must be based on four principles:

- Robust Fair Information Practices are the key to legislation concerning online privacy.
- Notice and choice are inadequate to protect consumers. Transparency is not enough if consumers have no real understanding or control.
- Self-regulation for privacy will not protect consumers.
- Law enforcement access to personal data should require a warrant.

The groups' detailed recommendations were spelled out in a recent letter to members of the House and I am including a copy of it for the record.

In conclusion, Web. 2.0 techniques offer government agencies powerful and valuable tools. They should be used carefully, however, without unduly favoring a particular provider and there must be explicit warnings when a consumer leaves an official government site. Most importantly, however, Congress must enact meaningful privacy legislation to safeguard consumers as they use these online services that have become known as Web 2.0. I look forward to your questions.