

**From:** Gil Silberman

**Sent:** Thursday, February 14, 2008 3:23 PM

**To:** BehavioralMarketingPrinciples

**Subject:** Public comment, project #P859900 ("Online Behavioral Advertising")

Dear Commissioners,

Please accept the attached letter as my company's response to the call for public comments regarding uses for tracking data other than targeted advertising, as well as the nature of "sensitive" data.

Let me know if the .pdf format I've used is acceptable or if there are any other concerns. I would be interested in following and helping with any further development of the proposal, so please feel free to contact me and use me as a resource on this and related matters.

Thanks,

G. Silberman

---

Gil Silberman  
Chief Legal Officer  
peerFluence, Inc.  
100 Pine Street  
Twenty Seventh Floor  
San Francisco, CA 94111

Gil Silberman  
Chief Legal Officer  
peerFluence, Inc.  
100 Pine Street, Twenty-Seventh Floor  
San Francisco, California 94111

February 14, 2008

Secretary, Federal Trade Commission  
Bureau of Consumer Protection  
600 Pennsylvania Ave., NW  
Room H-135 (Annex N)  
Washington, DC 20580

via electronic mail, BehavioralMarketingPrinciples@ftc.gov

Dear Commissioners,

My company, peerFluence, Inc., studies interactions among consumers on social media sites such as MySpace and Facebook, in order to understand how relationships among peers affect customer loyalty. We market our results to brand owners, content publishers, and the sites themselves. As Chief Legal Officer of the company I regularly address matters of privacy and consumer rights.

We are a step removed from advertising, but would like to share our experiences with other benign uses for behavioral tracking data, some of which may be considered “sensitive” per the Commission’s understanding. We applaud the Commission and the “Behavioral Advertising” participants for efforts to put online consumer information squarely in the hands of the consumers themselves. The proposed framework is a good start. Following are some further observations, and some proposals of our own for consideration.

### **Social media versus traditional services**

Traditional Internet services operate fairly anonymously. They offer content and services, and employ cookies and logon account registrations to correlate the activity of site visitors with their identity as consumers. The data is used to target advertising content to site visitors based on the aggregate behavioral demographics of consumer groups, and sometimes to direct ads to specific users who have been tracked from location to location on the Internet. Though ubiquitous, the practice is transparent to consumers, affecting them indirectly by affecting advertising rates charged for various parts of a publisher’s inventory, as well as offers that may be presented to online shoppers.

Consumers often do not know they are being silently observed or their information used, absent a regime of consent and disclosure. This raises questions of privacy and data security, and also of who owns the data and who is entitled to make decisions on what to do with it. To date the practice is considered benign mostly, with some concerns over identity theft and other privacy and security issues, as well as whether it is appropriate to use certain sensitive information (e.g. illness or other personal matters) as a criterion for serving ads.

Social media services (social networks, blogs, photo sharing, video exchange, and other participatory sites) are content sites that add an extra layer of sharing, personal reputations, and interpersonal relationships. With these new features the experience is far from anonymous. Information is explicitly provided by consumers, and generated by their daily social interactions, to a level of scope and detail far beyond traditional Internet sites. People are keenly aware they are creating a rich public

impression of who they are and what they are doing, but not always aware that advertisers are using the new information for their own purposes. Individuals announce on their profile pages where they live, their likes and dislikes, and their “social graph” of friends and colleagues. They post questions and give answers, write reviews of businesses and products, voice their opinions, and leave messages and endorsements on “walls” of others. They install “widget software” sponsored by companies and invite their friends to also install the widgets, become “fans” of their favorite music, films, and celebrities, share news and product information, exchange email and messages, and extend and receive invitations to events. This bundle of social interaction features, taken together, is a valuable new resource that creates advertising opportunities for social websites, the potential of which fuels “Web 2.0”, one of the liveliest and most promising of America’s emerging technology industries.

In addition to public information, social sites collect information they need to function but that is inherently private, such as email addresses, private communications, purchase history, credit card information, shipping address, and so on. They may also collect the same information as conventional passive sites such as page view and “click stream” records.

The new social media information is “tracking” data in the sense described by the Commission because it is personally-identifiable information about their online behavior. The difference is that consumers know their information is public, either desire or at least accept that they are making public disclosures, and are often the ones in control of the settings that turn the privacy switch on and off.

#### **Users want to share data**

On social media sites consumers purposely share their personal information, either to the public or among categories of people and businesses. They intentionally declare an online identity, find and keep track of friends, and carry out daily social interactions, knowing that network servers are storing the information so that the web service can run.

Behavioral scoring of consumers on social networks is no secret, and automates the very normal human process by which people affirm friendships, learn whose opinion they value, and decide who they can count on. Tracking data is collected, evaluated, and scored by the networks and third parties to create “trust” or “reputation” ratings that reward power users based on how many friends they have, how popular they are, how productive things they have done online, and how many people read and act on what they write. People leave personal or professional endorsements for each other, and rate each other’s photographs and blog posts with thumbs up or down. Restaurant review services give higher weight to writers with many friends and popular reviews. Blog services (and the meta-services that index blog content) rate posts for their authors’ respect among readers. Some reward their most valuable consumers with “elite” status, akin to a gold card in a customer loyalty program run by an airline, grocer, or bookstore. Users strive for a higher recognition. The outcome is a weighting system that helps consumers make informed choices, from where to buy a hamburger or take a vacation, to who they might vote for in an upcoming election.

In this context, “sensitive data” takes on a special meaning. Among a consumer’s choices is whether or not to disclose relationship status and history, sexual orientation, religion, political beliefs, drinking and smoking habits, employment history, income, and other information of a highly personal nature. Although it raises concerns to collect this information without the consumer’s informed consent, it would be problematic (and perhaps even unconstitutional if mandated by a government agency) to prohibit a carrier from conveying this information at the request of adult consumers.

As people become familiar with these sites they decide their own comfort level. How much of themselves do they want to reveal? Do they want to share their online actions with the public, keep the information entirely private, or restrict information to friends and/or trusted third parties? How honest and straightforward will they be about who their real friends are, where they work, their life

history, and their personality? They decide what to share, knowing that the more they give the network, the more the network can give back to them.

Ideally, use of tracking data within social networks should be disclosed in a way that a reasonable new user can figure it out. In our experience the more informed the consumer, the more likely they see reasonable use of personal data as benign, and will agree to provide fuller and more truthful personal information in exchange for better functionality. Experienced users, particularly younger adults, know what they are doing and have made their choices. An educated consumer base and vigilant consumer rights groups in turn help spot privacy and security flaws, and identify companies that are less than fully ethical in their use of data. New users, by contrast, are often unaware of the consequences of different privacy settings, or even that they have a choice.

A good historical comparison is phone numbers, where people make decisions on maintaining listed versus unlisted numbers, separate private numbers, whether to list cell phone numbers, and so on. Many were initially skeptical of caller ID features introduced in the early 1990s, but quickly accepted the benefit of announcing themselves when placing calls. FTC's Do Not Call Registry facilitated the new technology, along with other efforts to ensure that consumers were protected when disclosing private information. The issue here is that people chose their own level of privacy and the carriers, with the backing and support of the FTC, kept their information in a consistent, trustworthy manner that addressed any fear of abuse. A "Do Not Track Registry" may or may not be practical to implement online, but whatever the specifics, industry cooperation to and government support can give consumers the comfort they need to trust social media with their private data, thereby allowing the new technologies to reach their full potential.

### **Networks as public utilities**

Facebook, possibly the fastest-growing social network of the moment, famously calls itself a "social utility" for connecting people. We agree that the company and its peers are in some ways like telephone, transportation, and other carriers that link people together. Like these public utilities, social networks provide a global, ubiquitous, uninterrupted, nondiscriminatory, content-neutral infrastructure to connect people. In this conception, each person's login screen is like a dial tone, and their social graph is essentially their online rolodex, speed dialer, birthday minder, email organizer, and note-keeper.

As with other utilities, the parties at either end of the line may be individual consumers but they may also be business customers. For hotels, airlines, bookstores, and other enterprises, social networks are an effective new way to interact with consumers. Customers evaluate and buy products and services through social networks, create shopping "wish lists", receive invitations and coupons, chat with business representatives, obtain product support, pay bills, and write reviews and opinions of vendors, using the network platform as a medium of communication. To businesses a social utility becomes a worldwide marketplace, branding exercise, and suggestion box, all in one. These interactions do not originate from a specific social network any more than a person's mail order shopping or airline flight reservation comes from a single phone company or parcel service. Rather, there is a lifelong relationship between consumer and brand, with each network being a single modality consumers choose from time to time for communication.

### **Consumer needs**

Storing personal data is the defining feature of social networks, not just a byproduct useful for advertisers. Most would agree that the consumers themselves, not the website, inherently own the details of their personal lives, and that the consumer should therefore be the one in control that data. Keeping it secure and private is a crucial consumer protection, but so too is providing information back to the consumer or a trusted third party service if asked.

No personal computer owner doubts that their installed software will store the information they type in, keep it private, output it to paper or electronic file when the user needs it, and delete it on demand. The usefulness of the software, and therefore the fortunes of the company that publishes it, turns on consumers trusting that it will reliably perform these functions. It would be astonishing for a word processor, email client, or photo viewer to categorically refuse to send a consumer's desktop document out by email, citing privacy reasons or a proprietary business interest. Yet the issue is not clear when one moves the storage location from a consumer's desktop to the social media service's server farm. When customers upload their personal photos to a website they expect to download and share them on demand. When they key personal details into their online profile they expect the information belongs to them. However, some social networks prohibit, or take technological steps to prevent, users from freely sharing social graph and other account data. Expectations are not fully set. Whether data files will be portable as they are on the desktop is undecided, up to business competition and self-regulation on the part of industry.

Consumer groups advocate for privacy, security, consent, and disclosure with respect to private personal data. Increasingly, some promote the position that consumer data should be portable at the consumer's request, and interoperable with other software applications. They ask social media companies to interconnect their systems or else allow third party intermediaries to do so, in order that the online profile, reputation, social graph, and other data consumers and retailers invest time and money to create is not lost every time, but rather may be carried like a pen drive or appointment book from place to place at the user's request. Important providers such as Microsoft, Facebook, Yahoo!, and google, have recently joined efforts to develop data portability standards, working with groups such as dataportability.org (<http://www.dataportability.org>). They believe the industry will benefit if companies agree on common principles not only for privacy but also for data sharing at the request of users. On an individual level, consumers vote with their keyboards, mice, and credit cards for a right of privacy, and the freedom to communicate and interact as they wish. In other words they join the services they trust. If a service does not give them the assurances they want, and the matter is sufficiently important to them, they will find another provider.

## **Recommendations**

Our company's approach to privacy is simple. We follow best practices with respect to conventional tracking data where there are already industry norms. When new social media technologies bring new types and uses of data, the default position is to let consumers make informed choices without undue constraint for which services they choose and how they will use those services. Our default position for social network data used for any new third party purpose outside of the operation of the network itself is to work only with users who agree to take part, avoid storing information long-term, use information in aggregate rather than personally-identifiable form wherever possible, disclose results only with permission, and respect that every individual owns the facts of his or her own life.

Based on the foregoing we believe companies should self-regulate on the following principles:

- Personally-identifiable information entrusted to online social media services by their consumers should belong to the consumers themselves.
- Ownership of personal information implies not only a right of privacy but also a right to inspect and share the information. A social network carrier should not unreasonably refuse to deliver consumer information to the consumer or a trusted third party at the request of the consumer.
- Some interactions on social networks are a private matter between two people, or between a person and a company other than the host network. Social networks, acting as common carriers, should respect the privacy, sharing, and security instructions of the parties involved,

much as package delivery services or telephone companies respect the delivery specifications given by their customers.

- Strong, consistent, well-understood information policies benefit consumers, enterprises, and network carriers alike, and require consent and disclosure.
- Relationships among people, organizations, and companies, belong to the people involved and should not be hindered. If two parties choose one network over another for carrying on their relationship, networks should allow them to use the carrier of their choice without undue restrictions, rejection, or favoritism (but subject to technical limitations).
- Any system that regulates “tracking information” should recognize that it comes in several flavors. Some is already public, or covered by existing laws or contracts, and is beyond any further regulatory restriction. Users deliberately choose to disclose other information, and neither the consumers nor the social networks should be unduly hindered in fulfilling this consumer choice by rules that are ostensibly meant to protect the consumer. Yet other information is inherently private but necessary for social networks to operate. Gathering and using this information internally by the service itself should be encouraged, while establishing strong, consistent, rules regarding the type of consent required before sharing it with other parties.
- There are details to work out on which information is inherently public versus private, which information belongs to whom, what defines a reasonable request for privacy or sharing, what privacy and sharing choices should be offered, and the type of disclosures that should be offered to consumers.

## **Conclusion**

We hope the Commission recognizes that as one of the most promising sectors of the economy, America’s Internet industry deserves government support and encouragement. For their part companies like Microsoft, google, Facebook, and hundreds of smaller and newer participants are working on principles for privacy, security, consent, portability, and interoperability. We expect the outcome to favor consumer rights because empowerment benefits users, networks, and advertising constituents alike. The result will be self-regulation, expressed not only as public statements but also private contracts and practical cooperation among the parties involved. Any effort by the FTC to support this consensus is most appreciated.

Sincerely,

/s/ Gil Silberman  
Chief Legal Officer  
peerFluence, Inc.