From: Melissa Ngo, Privacy Lives Date: November 5, 2009
To: Federal Trade Commission
RE: Privacy Roundtables – Comment, Project No. P095416

Introduction

These comments concerning consumer privacy are submitted to the Federal Trade Commission ("FTC" or "Commission") as part of the Dec. 7, 2009 Privacy Roundtable discussion. In its notice, the FTC explained that it sought "to explore the privacy challenges posed by the vast array of 21st century technology and business practices that collect and use consumer data."[1] Below is a discussion about consumer privacy as applied to social-networking sites and the use of targeted behavioral advertising by the sites and third-party developers.[2] Though the discussion focuses on Facebook, the questions raised are applicable to all social-networking sites.

Fundamentally, the problem is that social-networking sites' business models require that members disclose as much data as possible in order to promote the "social" aspect of the company. Therefore, there is a business incentive for social-networking sites to weakly protect privacy while claiming to have strong consumer privacy protections to safeguard their public image.

The Federal Trade Commission has taken steps to strengthen consumer protection by investigating the online marketing industry and its behavioral profiling practices, holding a two-day town hall meeting on these issues in November 2007, as well as releasing improved self-regulatory principles.[3] Also, recently, some members of the online marketing industry agreed to self-regulatory

---

[1] *Fed. Trade Comm'n, Exploring Privacy: A Roundtable Series,* http://www.ftc.gov/bcp/workshops/privacyroundtables/index.shtml.

[2] For a framework and recommendations concerning protecting consumer privacy, see Ten Consumer Advocacy Groups, *Legislative Primer: Online Behavioral Tracking and Targeting Concerns and Solutions from the Perspective of Consumer Advocacy Groups* (Sept. 2009), *available at* http://www.privacylives.com/wp-content/uploads/2009/09/onlineprivacylegprimer_0909.pdf. This group includes Privacy Lives.

[3] FTC, *FTC Staff Report: Self Regulatory Principles for Online Behavioral Advertising* (Feb. 12, 2009), *available at* http://www2.ftc.gov/os/2009/02/P085400behavadreport.pdf (viewed Oct. 30, 2009).

principles, but as we will explain below, the industry has merely codified its current practices rather than improved consumer privacy protection.[4]

When the FTC released improved self-regulatory principles in February, Chairman Jon Leibowitz said, "Industry needs to do a better job of meaningful, rigorous self-regulation or it will certainly invite legislation by Congress and a more regulatory approach by our Commission."[5] For a variety of reasons, we believe industry self-regulation has failed to solve the problems connected with targeted online behavioral advertising, especially as connected with social-networking sites.

Therefore, the time has come for the FTC to consider more regulatory action. The FTC should act now to protect consumers and create regulations for data collection and use by the online marketing industry (which can include social networking sites), with strong penalties for noncompliance.

I. Industry Self-Regulation Has Not Worked to Improve Consumer Knowledge or Understanding of Targeted Online Behavioral Advertising

In an August 2009 interview with the *New York Times*, FTC Bureau of Consumer Protection Director David Vladeck said, "I'm a lawyer, I've been practicing law for 33 years. I can't figure out what the hell these [notice and consent disclosure forms] mean anymore. And I don't believe that most consumers either read them, or, if they read them, really understand it."[6] This is a clear statement of what we have known for years: Industry self-regulation has not improved consumer knowledge or understanding of targeted online behavioral advertising and the data collection done by the online marketing industry.

In the same interview, Vladeck said, "Until I see evidence otherwise, we have to presume that most people don't understand, and the burden is going to be on

---

[4] Interactive Advertising Bureau, *Self-Regulatory Principles for Online Behavioral Advertising* (July 2009) (hereinafter "Industry Self-Regulatory Principles"), *available at* http://www.iab.net/media/file/ven-principles-07-01-09.pdf (viewed Oct. 30, 2009).
[5] Jon Leibowitz, FTC Chairman, *Concurring Statement of Commissioner Jon Leibowitz: FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising* (Feb. 12, 2009), *available at* http://www.ftc.gov/os/2009/02/P085400behavadleibowitz.pdf (viewed Oct. 30, 2009).
[6] Editors, *An Interview With David Vladeck of the F.T.C.*, N.Y. TIMES, Aug. 5, 2009, *available at* http://mediadecoder.blogs.nytimes.com/2009/08/05/an-interview-with-david-vladeck-of-the-ftc/ (viewed Oct. 30, 2009).

industry to persuade us that people really are well informed about this."[7] There are numerous studies that show Vladeck is correct.

Surveys by the University of Pennsylvania's Annenberg School of Communication and the University of California at Berkeley Law School's Samuelson Law, Technology & Public Policy Clinic have found confusion about customer data and customer privacy protections offered by businesses. A September 2009 study by the universities revealed consumer confusion about how, when or if their data is protected. "Americans mistakenly believe that current government laws restrict companies from selling wide-ranging data about them. When asked true-false questions about companies' rights to share and sell information about their activities online and off, respondents on average answer only 1.5 of 5 online laws and 1.7 of the 4 offline laws correctly because they falsely assume government regulations prohibit the sale of data."[8]

This 2009 study follows surveys by the same universities conducted in 2007, which found confusion about companies' collection and use of customer data, and customer privacy protections offered by businesses. The surveys "indicate that when consumers see the term 'privacy policy,' they assume the website cannot engage in many practices that, in reality, are common in ecommerce. Consumers do not understand the nature and legality of information-collection techniques that form the core of online advertising business models."[9]

Some highlights from the 2007 surveys:

- "37% of online shoppers falsely believe that a privacy policy prohibits a website from using information to analyze individuals' activities online – a practice essential to most online advertising efforts."[10]

---

[7] *Id*.
[8] Univ. of Penn., Univ. of Cal. at Berkeley, *Americans Reject Tailored Advertising and Three Activities that Enable It,* 3, Sept. 2009 (hereinafter "Penn-Berkeley Study"), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214 (viewed Oct. 30, 2009).
[9] Joseph Turow, Deirdre K. Mulligan & Chris Jay Hoofnagle, Univ. of Pa.'s Annenberg Sch. for Commc'n & U.C.-Berkeley Law's Samuelson Law, Tech. & Pub. Policy Clinic, *Research Report: Consumers Fundamentally Misunderstand The Online Advertising Marketplace*, 1, Oct. 2007, (hereinafter "Annenberg/Samuelson Online Ad Surveys") *available at* http://groups.ischool.berkeley.edu/samuelsonclinic/files/annenberg_samuelson_advertising.pdf (viewed Oct. 30, 2009).
[10] *Id*. at 2.

- "55% (of respondents) either don't know or falsely believe that privacy policies prohibit affiliate sharing."[11]

- "55.4% agreed with the false statement that, 'If a website has a privacy policy, it means that the site cannot sell information about your address and purchase information to other companies.'"[12]

- 39.8% believed that "If a website has a privacy policy, it means that the site cannot buy information about you from other sources to analyze your online activities"[13]

Note that the 2007 report found, "When these techniques and the business model of online advertising are explained to them, [consumers] reject the privacy tradeoff made for access to content."[14] The 2009 report found, "when Americans are informed of three common ways that marketers gather data about people in order to tailor ads … between 73% and 86% say they would not want such advertising."[15]

Also, a 2008 survey from Consumer Reports showed that there is confusion among consumers about companies' privacy policies and practices.[16] Consumer Reports found: "61% are confident that what they do online is private and not shared without their permission"; "57% incorrectly believe that companies must identify themselves and indicate why they are collecting data and whether they intend to share it with other organizations"; and, "43% incorrectly believe a court order is required to monitor activities online."[17]

II. Marketing Industry Self-Regulation Will Not Work to Improve Consumer Privacy Protection

The online marketing industry has pointed to new self-regulatory principles, released in July, which the industry says shows an effort to improve consumer

---

[11] *Id*.
[12] *Id*.
[13] *Id*.
[14] Annenberg/Samuelson Online Ad Surveys, *supra* note 9 at 1.
[15] Penn-Berkeley Study, *supra* note 8 at 2.
[16] Consumers Union, *Consumer Reports Poll: Americans Extremely Concerned About Internet Privacy* (Sept. 25, 2008), *available at* http://www.consumersunion.org/pub/core_telecom_and_utilities/006189.html (viewed Oct. 30, 2009).
[17] *Id*.

privacy protection by following the FTC's recently promulgated self-regulatory principles.[18] However, for several reasons, these industry-imposed self-regulatory principles do little to protect consumer privacy. These problems unfortunately show that the FTC's self-regulatory principles have not worked to convince the online marketing industry to improve its consumer protections, and the FTC needs to step in to regulate the industry.

The only change of note in the industry self-regulatory principles seems to be an "enhanced notice" proposal. "Links to consumer notices will be clear, prominent, and conveniently located," for any businesses that voluntarily follow these principles.[19] Though we support improved transparency, this is not enough. The online marketing industry is merely providing an easier way for consumers to reach long and difficult-to-understand notices. Unless the notices are easier to understand, it will not matter if there are larger links to them on Web sites. Before any consumer data is collected, the users need to be candidly informed about the process – how their profile is created; how their profile evolves as more personal data is collected; how tracking and data gathering occurs site to site; and what data can be added to their profile from outside databases.

Another failure of the industry self-regulatory principles is its narrow definition of "sensitive data." The principles ask industry members not to collect "sensitive data," which the industry construes as (1) "personal information" of children under age 13 and (2) "financial account numbers, Social Security numbers, pharmaceutical prescriptions, or medical records about a specific individual."[20] The principles do allow for the collection and use of the second category – health and financial data – if a user consents to the collection and use.[21] This would permit widespread data collection involving personal information regarding our health and financial concerns based on consent that is gathered via complicated privacy notices and the user consent is most likely to be unknowing or confused.

---

[18] Industry Self-Regulatory Principles, *supra* note 4.
[19] *Id*. at 5.
[20] *Id*. at 16-17.
[21] *Id*. at 17.

The final and most important point where the industry's self-regulatory principles fails is enforcement. There is no enforcement provision. Non-compliance merely results in "public reporting" of non-compliance.[22] Companies could ignore the principles wholesale without facing meaningful penalties. Clearly, the industry's new self-regulatory principles are merely for public relations, rather than consumer protection.

III. Consumers Are Confused About the Privacy Policies and Data Collection of Social Networking Sites, Such as Facebook, and the Sites' Third-party Application Developers

A report released this year by the Office of the Privacy Commissioner of Canada studied six social networking sites: 1. Facebook (http://www.facebook.com) 2. Hi5 (http://hi5.com) 3. LinkedIn (http://www.linkedin.com) 4. LiveJournal (http://www.livejournal.com) 5. MySpace (http://www.myspace.com) 6. Skyrock (http://www.Skyrock.com).[23] The privacy office found that many social networking sites share the same problems concerning how and what they tell users about data collection and data sharing, and users' incomplete understanding of the sites' privacy policies. "Although the privacy policies of each of the sites acknowledged that information would be used in some way for advertising, none of them provided a clear statement of what information would be used, nor of how it would be shared. Sites were more likely to state that they would not share particular items of personally identifiable information (name, email, etc) than to list what information could or would be shared."[24] The report does note that some sites may have changed their policies since the report was issued.

We will focus on Facebook as an example of social networking sites with these problems. This was not the first time users' understanding of Facebook's policies had been questioned. A 2005 study by MIT student researchers found that,

---

[22] *Id*. at 18.
[23] Office of the Privacy Comm'r of Canada, *Social Network Site Privacy: A comparative analysis of six sites* (Feb. 2009), *available at* http://www.priv.gc.ca/information/pub/sub_comp_200901_e.pdf (viewed Oct. 30, 2009).
[24] *Id*. at 42.

in their survey of Facebook users, "46% of Facebook users believed that Facebook could not share their information with third parties."[25]

Facebook has created a unique space in the social networking world. It encourages users to share a significant amount of personal information in return for the benefits that Facebook provides including connecting with friends, sharing photos, publicizing events, and numerous others.

There are numerous third-party applications on Facebook. The social networking site says there are:

- More than one million developers and entrepreneurs from more than 180 countries;
- Every month, more than 70% of Facebook users engage with Platform applications;
- More than 350,000 active applications currently on Facebook Platform; and,
- More than 250 applications have more than one million monthly active users.[26]

According to Facebook, these applications "range from simple applications created by single users to share with their friends to impressive businesses employing hundreds of people and reaching tens of millions of users every month and generating tens of millions of dollars of revenue."[27]

Facebook requires users to register with a real name and to maintain current and accurate contact information.[28] Facebook's Privacy Policy focuses on the importance of privacy settings set by individual users and the policy itself is accessible from a link on the bottom of every page on the site. However, evidence shows that consumers are confused about the privacy policies and data collection practices of Facebook and its third-party application developers.

---

[25] Harvey Jones & Jose Hiram Soltren, *Facebook: Threats to Privacy* 23 (Dec. 14, 2005).
[26] Facebook, Press Room: Statistics, http://www.facebook.com/press/info.php?statistics (viewed Oct. 30, 2009).
[27] Facebook Developer Blog, *Happy 2nd Birthday, Facebook Platform!* (June 3, 2009 at 10:29 p.m.), http://developers.facebook.com/news.php?blog=1&story=252 (viewed Oct. 30, 2009).
[28] Facebook Homepage, http://www.facebook.com (viewed Oct. 30, 2009).

While Facebook users do exercise some control over the information they share with other users and applications, the default settings create an opt-out policy exposing extensive amounts of user information. Also, an individual user has to jump through a number of hoops to see all of the privacy options on Facebook, making it difficult to truly understand the social networking site's policies.

In a recent study of 45 social networking sites, researchers Joseph Bonneau and Soeren Preibusch of Cambridge University found that "Facebook had the most complex settings, with 61 options to select spread across 7 different privacy settings pages."[29] This is an overwhelming amount of information for users to sift through and makes it difficult for consumers to understand the implications of their choices.

In reviewing the 45 social networking sites, including Facebook, the researchers also found that "between 80 and 99% of users are typically found to never change their privacy settings."[30] Users are not opting out of default privacy settings, bringing into question the virtue of the opt-out standard when site defaults give developers access to much user data. There is also the concern that if so few users are changing their privacy policy, then either they do not understand the implications of retaining the defaults or how to find the settings necessary to change the data sharing.[31]

By default, Facebook makes it difficult for individuals to control who can see, collect or use their personal data. This creates substantial consumer confusion about users' data privacy rights and about the data collection and use by Facebook and its third-party application developers.

IV. Some Social-Networking Sites' Policies, Including Facebook's, Do Not Adequately Protect Consumer Privacy

There is evidence that shows some social-networking sites' policies do not adequately protect consumer privacy. Again, we turn to Facebook as an example.

---

[29] JOSEPH BONNEAU & SÖREN PREIBUSCH, THE PRIVACY JUNGLE: ON THE MARKET FOR DATA PROTECTION IN SOCIAL NETWORKS 19 (2009) (hereinafter "Bonneau & Preibusch"), *available at* http://preibusch.de/publications/Bonneau_Preibusch__Privacy_Jungle__2009-05-26.pdf (viewed Oct. 30, 2009).
[30] *Id*. at 18.
[31] *Id*. at 19.

From what is visible on the Facebook site to users, Facebook, developers and users simply appear to be connected. Lurking below the surface, however, is an entire service and support system for third-party application developers to track and collect data from users to enhance user engagement with applications. Facebook has more than 300 million active users and more than 70 percent of Facebook users interact with Platform applications every month.[32] Facebook reports that the average user has 130 friends and there are more than 45 million status updates each day.[33]

A. Facebook's Governing Documents Are Confusing to Consumers and Unfairly Place Burden on Consumers

The governing Facebook documents and contracts that make up a confusing web of duties and responsibilities include the Principles, Statement of Rights and Responsibilities, Privacy Policy, Platform, and the Developer Principles and Policies. These governing documents contain powerful language about protecting user privacy, yet these same documents relinquish all responsibility for actions of third-party application developers, as we explain below.

When viewing the Facebook Principles, we find a general problem: There is substantial use of "should," which implies a choice on Facebook's part whether or not to follow these Principles.[34] The use of "should" allows Facebook to use these Principles as public relations camouflage while retaining legal wiggle room to ignore the Principles completely.

The Facebook Privacy Policy broadly states how user data will be shared.[35] "We share your information with third parties when we believe the sharing is permitted by you, reasonably necessary to offer our services, or when legally required to do so."[36]

---

[32] Facebook, Press Room: Statistics, *supra* note 26.
[33] *Id.*
[34] Facebook, Site Governance: Facebook Principles (April 15, 2009), http://www.facebook.com/note.php?note_id=183540865300 (viewed Oct. 30, 2009).
[35] Facebook, Privacy Policy (October 29, 2009), http://www.facebook.com/note.php?note_id=%20322194465300 (viewed Oct. 30, 2009).
[36] *Id*.

Research reveals that "reasonably necessary to offer our services" has, in practice, been over-inclusive. Applications are a dominant presence on Facebook and have used the default privacy settings to their advantage to collect as much data as possible from the platform – "public" (such as users' names or lists of friends) and "private" (such as users' birthdays) Facebook information. A 2007 University of Virginia report on third-party applications found that, of the top 150 applications on Facebook, 8.7 percent did not require any user data, 88.7 percent used public information and only 9.3 percent needed private data.[37] The study's co-author Adrienne Felt explained in a news interview, "Since all of the applications are given full access to private data, this means that 90.7 percent of applications are being given more privileges than they need."[38]

Facebook denies responsibility for third-party application developers' compliance with the developers' own contracts: "We do not own or run the applications and websites that you interact with through Facebook Platform, and while we try to enforce standards to protect your information, we cannot guarantee that they will follow our rules."[39] This raises the question: On what information do Facebook users base their decision to use Facebook and its applications? Is the decision based on what users see on Facebook's myriad pages containing references to privacy or on the third-party developers' Web sites? This unfairly places the burden on consumers to cross reference a confusing set of documents when trying to make decisions about the privacy of their data.

B. Facebook Is an Example of a Social-Networking Site That Has Not Proved Systemic Screening or Auditing of Third-Party Application Developers

We have found that some social-networking sites do not have systemic screening of auditing of their third-party application developers. Facebook has

---

[37] Adrienne Felt and David Evans, Univ. of Va., *Privacy Protection for Social Networking APIs* (Oct. 2007), *available at* http://www.cs.virginia.edu/felt/privacybyproxy.pdf (viewed Oct. 30, 2009).
[38] Chris Soghoian, *Exclusive: The next Facebook privacy scandal*, CNET NEWS, Jan. 23, 2008, http://news.cnet.com/8301-13739_3-9854409-46.html (viewed Oct. 30, 2009).
[39] Facebook, Facebook Platform (August 28, 2009), http://developers.facebook.com/user_terms.php (viewed Oct. 30, 2009).

recently created the "Application Verification Program," where third-party application developers can voluntarily undergo a review by Facebook. According to Facebook, "Verified applications have passed a detailed Facebook review to confirm that the user experience they provide complies with Facebook policies. Verified applications have committed to be transparent about how they work and will respect you and your friends when they send communication on your behalf."[40] If Facebook evaluated the applications and is willing to add a tag such as "Verified Application," then these applications would be presumed to follow Facebook's stated privacy standards, which the company maintains are strong and user-protective. This raises the question: If Verified Applications have passed Facebook screening, then what about the rest of the more than 350,000 active applications currently on Facebook Platform?

In a recent investigation of Facebook, the Privacy Commissioner of Canada said that, after reviewing Facebook policies and speaking with company representatives, "Facebook has provided no evidence that it systematically screens or audits the activities of application developers. Rather, it relies primarily on users themselves to identify developers that may be violating the [Statement of Rights and Responsibilities] and Platform Guidelines."[41] The report also said, "Most notably, regarding third-party applications, the Assistant Commissioner determined that Facebook did not have adequate safeguards in place to prevent unauthorized access by application developers to users' personal information, and furthermore was not doing enough to ensure that meaningful consent was obtained from individuals for the disclosure of their personal information to application developers."[42] In fact, the

---

[40] Facebook, Help Center: General Application Support: Application Directory, *available at* http://www.facebook.com/help.php?page=876 (viewed Oct. 30, 2009).
[41] Elizabeth Denham, Assistant Privacy Commissioner of Canada, *Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. under the Personal Information Protection and Electronic Documents Act* 42 (July 16, 2009) (hereinafter "Canada Report on Facebook"), *available at* http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.cfm (viewed Oct. 30, 2009). The original complaint the Privacy Commissioner's investigation was based on was filed by the Canadian Internet Policy and Public Interest Clinic ("CIPPIC") in May 2008, *available at* http://www.cippic.ca/uploads/CIPPICFacebookComplaint_29May08.pdf (viewed Oct. 30, 2009).
[42] Canada Report on Facebook at 3, *supra* note 41.

Commissioner said, "In Facebook's opinion, it is in the developers' best interest to 'play nice' because it is the developers who have the most to lose if they do not respect the rules, given that many applications are commercial in nature and aim to generate traffic and serve ads."[43]

Conclusion

Social-networking sites and advertising and marketing companies will continue to be part of national and international media, and there are benefits to these businesses. However, as noted above, there can arise substantial threats to our privacy and related consumer protection issues in their business practices and policies. We must look closely at these businesses and strengthen consumer privacy protections.

Respectfully submitted,

Melissa Ngo
Privacy and Information Policy Consultant
Privacy Lives

P.O. Box 17035
Arlington VA 22216
privacy [at] privacylives.com
www.PrivacyLives.com

Submission date: November 5, 2009

[43] *Id*. at 42.