Before the

Federal Trade Commission

Washington, DC 20580

Comments of Guilherme Roschke,

Fellow, Institute for Public Representation,

Georgetown University Law Center

RE: Privacy Roundtables – Comment, Project No. P095416

This comment analyzes the shortcomings in the IAB's Self Regulatory Principles for Online Behavioral Advertising.[1] FTC staff requested information the adequacy of current protections in question #3:

> Do existing legal requirements and self regulatory regimes in the United States today adequately protect consumer privacy interests?[2]

[1] Interactive Advertising Bureau, *Self Regulatory Principles for Online Behavioral Advertising* (July, 2009), *available at http://www.iab.net/media/file/ven-principles-07-01-09.pdf* [hereinafter *IAB Principles*].

[2] Federal Trade Commission, *Exploring Privacy: A Roundtable Series*, http://www.ftc.gov/bcp/workshops/privacyroundtables/.

The IAB principles are of limited scope, offer ineffective transparency, limited consumer control and fail to adequately protect sensitive data. In regards to children's privacy and spyware, the principles amount to a promise to follow existing legal minimums – promises which should be a given in any self-regulatory scheme

I. THE IAB PRINCIPLES ARE OF LIMITED SCOPE

The first major flaw of the IAB principles is their limited scope. The IAB exempts first parties in a way that does not match consumer expectations. Further, the IAB principles do not protect consumers from third party tracking that comes with embedded content. Finally, the principles only apply to the collection *and* use of information online exempting information collection or information use or the use of offline data by themselves.

The IAB creates three categories of entities that engage in profiling: (1) "First Parties," exempt from the principles, are those engaging in profiling on their own websites, their agents and affiliates, and those profiling via embedded content;[3] (2) "Third parties" engaged in "Online Behavioral Advertising," to whom the principles apply, and does not include the agents of "first parties";[4] and (3) "Service Providers," which capture all or substantially all of the URLs viewed by a browser.[5] This latter category includes technologies such as Deep Packet Inspection and client side adware/spyware technologies. Service Providers face a stricter set of measures under the IAB principles.

---

[3] *IAB Principles, supra* note 1, at 10.
[4] *Id.* at 11.
[5] *Id.*

Broadly exempting first parties and their agents avoids covering a significant amount of profiling done on social network websites and other portals. Broadly exempting first parties also means that mergers between third parties and first parties will remove the third party data from the protection afforded by the principles. However, the FTC's proposed principles chose to exempt first parties for several reasons. The FTC staff concluded that first party profiling is more likely to be consistent with consumer expectations; first party collection and use may be necessary for beneficial consumer services, and maintaining data for internal use limits the risk that data will fall into the wrong hands.[6]

In contrast to the FTC's findings, the IAB's principles exempt first parties from the point of view of corporate ownership and control relationships. If first parties are to be exempted, they should be exempted from the point of view of the consumer and consumer's expectations of who they are dealing with. First parties should not be exempted based on complicated corporate structures and relationships that are opaque to users. Consumers have little to no knowledge of affiliate and control relationships behind different websites, domains and brand names. Business entities place several brands and identities before consumers for legitimate reasons such as creating different consumer expectations and different consumer experiences. A consumer that digs in and finds disparate and decentralized data collection from several brand names will not know that these are actually under the same corporate parent and sharing information.

Embedded content is also not protected. In the commentary, the IAB notes that in situations where it is "clear that the consumer is interacting with a portion of a web site that is

---

[6] Federal Trade Commission, *FTC Staff Report: Self Regulatory Principles For Online Behavioral Advertising*, 26-7, (February 2009), http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf.

not an advertisement and is being operated by a different entity than the owner of the website," then the entity embedding content would not be considered a third party for the purposes of the principles.[7] Since first parties are unregulated by the principles, this means that users who interact with (or are shown) embedded content will not receive protection from the principles.

The principles do not cover the practice of "enhancing" data with other sources, such as data broker databases of consumer information. Thus another scope limitation is in the definition of Online Behavioral Advertising. This is limited to collection *and* use of data for online marketing.[8] If the data is collected by some other means, or if the use is for something other than online behavioral advertising, then the principles will not apply.

II. THE IAB PRINCIPLES FAIL TO DELIVER SIMPLE TRANSPARENCY

The goal of transparency fails because consumers will continue to not know how they are being targeted on a given website. The IAB will not be providing one place where adherents to the principles offer their disclosures and offer an opportunity for consumers to exercise choice. Nor will the IAB be providing access to data collection that is as easy for consumers to perceive as the industry's ad-delivery and data collection system. The IAB's transparency principle describes several forms of notice that may be given by behavioral targeting companies within the scope of the principles. Placing a notice around the ad has the most promise in achieving transparency in these principles. However, the transparency principle envisions a world where all consumers would get after following several links is an industry website listing some, but not all, profilers with no hint as to which one has what information on the consumer.

---

[7] *IAB Principles, supra* note 1, at 24.
[8] *Id.* at 10.

Much of the transparency promised in the principles will depend on implementation. Questions such as how prominent links are, how explanatory, or whether they include words that lead consumers to mistakenly conclude they are protected, are not specified. Briefly, behavioral targeting third parties are required to maintain notices and a choice mechanism on their own websites.[9] However, consumers normally won't be browsing these third party websites – profiling is done by these third-parties while consumers are browsing other first-party websites. The principle requires third parties to individually participate in one of several other notice alternatives and each requires a link to the disclosure and choice mechanism on the third party website. [10] These are termed an "enhanced notice" in the principles: (1) a notice around the ad, (2) a notice on the web page where data is collected, (3) a listing on an industry developed website linked from a web site disclosure, or (4) an individual listing on a web site disclosure. The "website disclosure" refers to a disclosure on the first-party web site, linked from the pages where data is collected. This describes a world where a consumer being profiled at a given web page would also see on that page a link. This link would take them to the section of the first party's privacy policy discussing the behavioral profiling. This section would either link to the specific profiler's notice or to the industry generated website that lists all the participating profilers. The consumer would then have to navigate that industry developed website to find the profiler they are interested in – with no hint of who profiled them on the web page they came from -- follow that link, read the notice there, and exercise choice.

The goal of transparency thus fails. Behavioral targeting companies have several options of how to make their disclosures and how to offer consumers an opt-out. Consumers will have to

---

[9] *Id.* at 12.
[10] *Id.* at 13.

check several different sites, and follow different links, in order to find out whether they are targeted and how to opt out.

III. THE IAB PRINCIPLES OFFER LIMITED CONSUMER CONTROL

The IAB principles describe consumer control that has the potential to be as confusing as its transparency system, and, in the case of entities defined as "Service Providers," merely implements existing legal standards. The IAB principles describe two forms of consumer control to be applied to the collection and use of data for online behavioral targeting. Behavioral targeting third parties will provide "choice" linked from the notices described in the transparency principle.[11] Additionally, Service Providers will be required to get "Consent," and to offer a means for the withdrawal of Consent.[12]

The Behavioral targeting third parties are to offer the choice mechanism "either on its own website, on an industry developed website, or listed individually in the disclosure of the website where data is collected."[13] The actual technical implementation for choice is not specified. If this choice follows current opt-out schemes, it likely will involve the use of opt-out cookie or opt-out plugin.[14] Opt-out cookies are problematic because they are inconsistent with other recommended privacy practices such as blocking third party cookies and clearing cookies. Opt-out cookies may contain unique identifiers and allow for tracking. Further, the cookies may be set to expire prematurely and surprise consumers. The choice applies to the "collection *and*

---

[11] *Id.* at 14.
[12] *Id.*
[13] *IAB Principles, supra* note 1, at 34.
[14] *See*, Google, *Advertising Cookie Opt-out Plugin*, http://www.google.com/ads/preferences/plugin/; Network Advertising Initiative, *Opt Out of Behavioral Profiling*, http://www.networkadvertising.org/managing/opt_out.asp.

use" [emphasis added] of data for online behavioral advertising and for the transfer of data to non-affiliates for such purposes.[15] Other forms of choice, such as preventing the collection of data alone, or the use of data alone, will not be included. The collection and use or transfer of data for other purposes also will not be subject to choice. Consumers are also not able to exercise control over their data that is already collected by demanding that it be destroyed.

Service Providers, who collect all or substantially all of the urls a browser visits, will be required to get "Consent," before they can "collect and use" data for behavioral targeting. They should also offer a means for the withdrawal of Consent.[16] Per the definition, "Consent" means an "individual's action in response to clear, meaningful and prominent notice" of the collection and use of data.[17] This is further clarified as requiring that consumers "take action assenting to the collection and use of data."[18] This higher requirement is an effective opt-in for these services. Like the "choice" offered for other services, this one also limited to the junction of "collection *and* use." Further, the withdrawal of consent does not destroy the data, and does not prevent other uses besides online behavioral targeting.

The Service Provider level of disclosure and control is roughly equivalent to what the Federal Trade Commission considers a minimum to escape liability under its actions against spyware and adware companies. The FTC case against Odysseus Marketing, Inc charged as a deceptive trade practice the failure to disclose the "installation of additional software programs, some of which replace search results provided by search engine web sites, collect and transmit information from computers to third parties, send pop-up advertisements and other Internet ads,

---

[15] *IAB Principles, supra* note 1, at 14.
[16] *Id.*
[17] *Id.* at 10.
[18] *Id.* at 36.

and download more software programs."[19] In the case against Zango, Inc, the FTC charged as a deceptive practice that Zango and its affiliates "failed to disclose, or failed to disclose adequately, that the lureware was bundled with Respondents' adware that would monitor consumers' Internet use and cause consumers to receive numerous pop-up advertisements based on such use."[20] The case against Advertising.com charged as deceptive the practice of installing adware that:

> …collected information about SpyBlast users, including URLs of visited pages and the user's IP address, and this information allowed respondents to send users advertisements that respondents believed might be of interest to them. Consumers received a substantial number of pop-up advertisements as result of respondents' installation of this adware onto their computers.[21]

These entities are Service Providers under the IAB's definition – collecting and using data from all or substantially all of the urls a browser visits. These entities are charged with failing to make meaningful disclosures when consumers opt-in to install the software which performs the data collection and delivers ads. The IAB's requirement of clear, meaningful and prominent notice of these practices merely follows the minimums established in these FTC cases: that meaningful disclosures are required before consumers agree to services or software that will track all of the urls they visit and deliver ads based on these.

---

[19] *FTC vs. Odysseus Marketing, Inc*, Complaint at ¶ 30, (Sept. 21, 2005), http://www.ftc.gov/os/caselist/0423205/050929comp0423205.pdf.
[20] *In Re Zango Inc. f/k/a 180Solutions*, Complaint at ¶ 16, Docket No. C-4186, (March 7, 2007), http://www.ftc.gov/os/caselist/0523130/0523130c4186complaint.pdf.
[21] *In Re Advertising.com*, Complaint at ¶ 8, Docket No. C-4147 (Sept. 12, 2005), http://www.ftc.gov/os/caselist/0423196/050916comp0423196.pdf.

IV. THE IAB's "SENSITIVE DATA" INADEQUATELY PROTECTS CONSUMER INTERESTS.

The IAB's conception of "sensitive data" is limited and inadequate to the various categories of data that consumers deem "sensitive." Only a fraction of what consumers consider financial or health information is protected. With respects to children's data, the treatment is basically a promise to follow COPPA – with a caveat that shows the weakness in the IAB's definition of Personally Identifiable Information. Advertisers will still be able to collect information on, profile, and target children and minors beyond COPPA.

Under "Health and financial" data, the promise is to not collect and use "account number, social security numbers, pharmaceutical prescriptions, or medical records about a specific individual."[22] Other health and financial information, such as salary figures, account balances, retirement contributions, interest in medical ailments, medications and procedures, age, sexual orientation, or disability status would not be covered. Consumers who search or browse for important medical information will have this data collected and used for online behavioral advertising without their opt-in consent. Consumers searching for obesity, diet or nutrition information will also be potentially profiled in ads they receive. Likewise data can be collected and used to make inferences about consumers' sexual orientation, their gender, age, and financial condition.

The IAB simply promises to follow COPPA in its discussion of children's data as "sensitive." In discussing marketing to children, the Principles state:

---

[22] *IAB Principles, supra* note 1, at 17.

> Entities should not collect "personal information," as defined in the Children's Online Privacy Protection Act ("COPPA"), from children they have actual knowledge are under the age of 13 or from sites directed to children under the age of 13 for Online Behavioral Advertising, or engaged in Online Behavioral Advertising directed to children they have actual knowledge are under the age of 13 except as compliant with the COPPA.[23]

This is basically a promise to follow COPPA and should be a given in any self-regulatory regime. In order to promise to follow the law, the IAB needs to specify that the definition of personal information is from COPPA because the definition in COPPA is more expansive than the restrictive definition used by the IAB. The IAB definition is "information about a specific individual, including name, address, telephone number and email address – *when* used to identify a particular individual." [emphasis added][24] COPPA defines PII as "individually identifiable information" even when not used to identify someone.[25] Thus even its own definition of PII would not be COPPA compliant. The Principles need a special category and special treatment for children's data because they need another definition of PII in this section. No protection is offered to data on teens not covered by COPPA.

The principles leave open the possibility that behavioral marketing can be directed at the computer a child is using, so long as COPPA-defined PII on the child is not collected. Children will have their data collected and used for behavioral marketing when they are using websites that are not directed at children or where there is no actual knowledge that they are children and

---

[23] *Id.* at 16-17.
[24] *Id.* at 11.
[25] 15 U.S.C. § 6501(8).

COPAA-defined PII is not collected. Thus a child could be profiled as a child, there would be knowledge that data was being collected from a child and used to profile that child, but so long as there was no COPPA-defined PII collected, the principles would offer no "sensitive data" protection to that child. Further, data on teens 13 and over will be collected and used without requiring opt-in consent.

V. THE IAB's ACCOUNTABILITY PROMISE IS INCOMPLETE

The principles describe features that accountability programs should have, including monitoring, reporting, and compliance systems. [26] The accountability programs are promised to be in place by "the beginning of 2010".[27]

VI. CONCLUSION

The principles are of limited scope, offer ineffective transparency, limited consumer control and fail to adequately protect sensitive data. In regards to children's privacy and spyware, the principles amount to a promise to follow existing legal minimums. Such promises do not significantly advance consumer privacy.

Respectfully Submitted,

Guilherme Roschke
Staff Attorney / Fellow
Institute for Public Representation
First Amendment and Media Center
Georgetown University Law Center

[26] *IAB Principles, supra* note 1, at 17, 18.
[27] *Id.* at 41.

November 6, 2009.