

and some consumer groups cited potential harmful secondary uses, including selling personally identifiable behavioral data, linking click stream data to PII from other sources, or using behavioral data to make credit or insurance decisions. These commenters noted, however, that such uses do not appear to be well-documented. Some commenters recommended that the FTC seek more information regarding secondary uses, including the extent to which the collection of data by third-party applications operating on a host website constitutes secondary use.

Given the dearth of responses to staff's request for specific information, it is unclear whether companies currently use tracking data for non-behavioral advertising purposes other than the internal operations identified above.<sup>78</sup> Staff therefore does not propose to address this issue in the Principles at this time. Staff agrees with some of the commenters, however, that the issue of secondary use merits additional consideration and dialogue. Therefore, as staff continues its work on behavioral advertising, it will seek more information on this issue and consider further revisions to the Principles as needed.

#### **IV. REVISED PRINCIPLES**

Based upon the staff's analysis of the comments discussing the Principles as initially proposed, and taking into account the key themes enumerated above, staff has revised the Principles. For purposes of clarification, the new language is set forth below in bold and italics. As noted above, these Principles are guidelines for self-regulation and do not affect the obligation of any company (whether or not covered by the Principles) to comply with all

---

<sup>78</sup> Where companies are using tracking data for non-behavioral advertising purposes, such uses may involve sharing the data with third parties. If so, the notice and choice that a company provides concerning such sharing may address at least some of the concerns raised about secondary uses. A secondary use may also constitute a retroactive "material change" to a company's existing privacy policy, in which case consumers could choose whether to provide affirmative express consent to the change.

applicable federal and state laws.

**A. Definition**

For purposes of the Principles, online behavioral advertising means the tracking of a consumer’s online activities *over time* – including the searches the consumer has conducted, the web pages visited, and the content viewed – in order to deliver advertising targeted to the individual consumer’s interests. ***This definition is not intended to include “first party” advertising, where no data is shared with third parties, or contextual advertising, where an ad is based on a single visit to a web page or single search query.***

**B. Principles**

1. Transparency and Consumer Control

Every website where data is collected for behavioral advertising should provide a clear, concise, consumer-friendly, and prominent statement that (1) data about consumers’ activities online is being collected at the site for use in providing advertising about products and services tailored to individual consumers’ interests, and (2) consumers can choose whether or not to have their information collected for such purpose. The website should also provide consumers with a clear, easy-to-use, and accessible method for exercising this option. ***Where the data collection occurs outside the traditional website context, companies should develop alternative methods of disclosure and consumer choice that meet the standards described above (i.e., clear, prominent, easy-to-use, etc.)***

2. Reasonable Security, and Limited Data Retention, for Consumer Data

Any company that collects and/or stores consumer data for behavioral advertising should provide reasonable security for that data. Consistent with data security laws and the FTC’s data security enforcement actions, such protections should be based on the sensitivity of the data, the

nature of a company's business operations, the types of risks a company faces, and the reasonable protections available to a company. *Companies should also retain data only as long as is necessary to fulfill a legitimate business or law enforcement need.*

3. Affirmative Express Consent for Material Changes to Existing Privacy Promises

As the FTC has made clear in its enforcement and outreach efforts, a company must keep any promises that it makes with respect to how it will handle or protect consumer data, even if it decides to change its policies at a later date. Therefore, before a company can use *previously collected* data in a manner materially different from promises the company made when it collected the data, it should obtain affirmative express consent from affected consumers. This principle would apply in a corporate merger situation to the extent that the merger creates material changes in the way the companies collect, use, and share data.

4. Affirmative Express Consent to (or Prohibition Against) Using Sensitive Data for Behavioral Advertising

Companies should collect sensitive data for behavioral advertising only after they obtain affirmative express consent from the consumer to receive such advertising.

**V. CONCLUSION**

The revised Principles set forth in this Report constitute the next step in an ongoing process, and staff intends to continue the dialogue with all stakeholders in the behavioral advertising arena. Staff is encouraged by recent steps by certain industry members, but believes that significant work remains. Staff calls upon industry to redouble its efforts in developing self-regulatory programs, and also to ensure that any such programs include meaningful enforcement mechanisms. Self-regulation can work only if concerned industry members actively monitor compliance and ensure that violations have consequences.