

FTC BEHAVIORAL ADVERTISING PRINCIPLES

Proposed Principle (2008)	Proposed Principle Definition (2008)	New Principle (2009)	Notes
Definitions			<p>It's worthwhile to note that the FTC defines BA so as not to include "first party" (no data shared with third parties or only used within a single site or related group of sites), or what it calls "contextual advertising" (an ad is based on a single session at a web site or search query. Think of it as BA-lite.). The lesson here is that a business is generally free to use consumer data within its own site without concern of falling afoul of the Principles, and similarly may make use of basic, 'session' information (non-retained user data) also without concern over the Principles' applying.</p>
Transparency and consumer control	<p>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</p>	No changes.	<p>Maintaining a simple privacy disclosure page with a link to an opt-out page from BA data collection, if appropriately mentioned in a banner or 'home page', probably continues to be sufficient. Also, the notes suggest changes to a business' use of consumer data don't require notice to users unless the changes are <i>"material"</i>.</p> <p>Finally, several web sites (Yahoo, Google, and Double-Click for example) already have "opt-out" procedures.</p>

Proposed Principle (2008)	Proposed Principle Definition (2008)	New Principle (2009)	Notes
	purpose. The website should also provide consumers with a clear, easy-to-use, and accessible method for exercising this option.		Unfortunately, while these opt-out pages can be found without too much difficulty, some of them fail to disclose the fact that the opt-out procedure itself relies on cookies, and the next time a user cleans their cookies from their computer, they will in effect be automatically “opted-in” again. The FTC staff noted this concern amongst technical experts providing comments, but did not directly suggest companies needed to revise this process to make it more functional or transparent.
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 the 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 retain data only as long as is necessary to fulfill a legitimate business or law enforcement need.	No changes.	Reasonable security is as reasonable security does. The concept probably remains tied to whatever is the prevailing industry standard at the time. This is also the approach taken by many state data breach notification laws, some of whom levy an affirmative duty on businesses to maintain “reasonable security procedures and practices appropriate to the nature of the information” (California § 1798.81.5(b)). The question of retention though and legitimate business need suggests that companies may invent or discover new business needs, and as long as a new practice is disclosed, continue to retain consumer information indefinitely.

Proposed Principle (2008)	Proposed Principle Definition (2008)	New Principle (2009)	Notes
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 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.	<p>The phrase “previously collected” was insert in the sentence highlighted.</p> <p>Therefore, before a company can use <i>previously collected</i> 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.</p>	The FTC added “previously collected” data in this principle, to allow businesses to use newly acquired data without such restrictions. Generally, if a business collects data from you under a privacy disclosure statement that says it will not share that data with a third party, it cannot later change that disclosure and then share all the data it has accumulated on a user for the whole time he/she has been a customer, unless it gets that user’s affirmative express consent. However, if a business changes their disclosure policy to say they can now share data, they don’t have to get a user to expressly consent to this, as long as they only share new information they obtain <i>after</i> they make the change to the disclosure policy.
Affirmative express consent to (or prohibition against) using sensitive data for behavioral advertising	Companies should only collect sensitive data for behavioral advertising if they obtain affirmative express consent from the consumer to receive such advertising.	No changes.	No real definition is provided for “sensitive data”. A few examples include “financial data, data about children, health information, precise geographic location information, and Social Security numbers”. However, uses within a single site (not shared with a third party) of sensitive data without consent is not covered by the principles at all, and include “selling personally identifiable behavioral data, linking click stream data to PII from other sources, or using behavioral data to make credit or insurance decisions”.