



Comments of Shop.org,  
A division of the National Retail Federation,  
And the National Retail Federation  
Before the  
Federal Trade Commission  
On  
“Online Behavioral Advertising:  
Moving the Discussion Forward to Possible Self-Regulatory  
Principles”

**Elizabeth Oesterle**  
Vice President  
Government Relations Counsel  
The National Retail Federation

**Scott Silverman**  
Executive Director  
Shop.org

325 7<sup>th</sup> Street, N.W.  
Suite 1100  
Washington, D.C. 20004  
(202) 783-7971

## Introduction

Multichannel retailers have spent over a decade revolutionizing the way Americans shop by giving each and every consumer greater access to a wide variety of brands, goods, and services at highly competitive prices with the click of a mouse. Ecommerce has brought millions of new customers to retailers' virtual stores and has also served to increase new customer traffic in brick and mortar stores after browsing online. According to the Shop.org<sup>1</sup> annual study, *The State of Retailing Online* ("SORO"), conducted by Forrester Research, Inc., online retail sales soared to \$220 billion (including travel) in 2006, up 25 percent over 2005.<sup>2</sup> Excluding the travel category, business-to-consumer ecommerce in the United States reached \$146.5 billion in 2006, and jumped another 21 percent to \$175 billion in 2007<sup>3</sup>.

As multichannel retailers continue to fine-tune their online selling and marketing strategies, consumers have become more comfortable shopping online – especially with retailers that they know and trust. In 2006, online sales reached 7 percent of all retail sales.<sup>4</sup> In contrast, it took the catalog industry *100 years* to represent just 4.7 percent of retail sales.<sup>5</sup> What has made the retail Internet revolution possible is both the widespread access to the web and e-mail by American consumers *and* the ability for retailers to actively and nimbly adapt to their customers' evolving shopping preferences. Retailers are constantly re-designing and adding new features to their web sites; striving to create the most relevant

---

<sup>1</sup> Shop.org, a division of the National Retail Federation, is the world's leading membership community for digital retail. Founded in 1996, Shop.org's 700 members include the 10 largest retailers in the U.S. and more than 60 percent of the *Internet Retailer* Top 100 E-Retailers.

<sup>2</sup> The State of Retailing Online 2007, Part 1 of 2

<sup>3</sup> The State of Retailing Online 2008 as released on April 8, 2008. Totals including travel are not yet available for 2007.

<sup>4</sup> The State of Retailing Online 2007

<sup>5</sup> The State of Retailing Online 2002

content and consumer-friendly web experience that they can to maintain their customer base, draw in new shoppers, and improve overall conversion rates. In fact, retailers *have to be* relentless about delivering the most compelling and relevant experience to their customers because that is how they differentiate themselves in an extremely competitive environment.

The key to the constant evolution of retail sites is the knowledge that retailers have gained about their customers' shopping habits (or "behaviors") on their websites over time. In fact, one key finding of the *2007 SORO* survey is that retailers with an online presence for more than nine years were among the best performing segments with conversion rates approaching 4 percent, as opposed to a 2.8 percent conversion rate for companies that have been in business for 4 years or less.<sup>6</sup> Forrester Research, Inc., who conducts the *SORO* survey, attributes the success of more mature retail sites to the fact that, "they have a long history of experimenting in the channel and ... also have larger house files that they have cultivated over time, which naturally draws upon the channel's best customers."<sup>7</sup> Retailers have long understood that keeping their customers happy is the most essential part of building positive long-term business relationships. A satisfied customer is a repeat customer. That being said, retailers do not want to fundamentally alter an entire medium for effective information delivery just because a limited number of consumers, mostly represented by groups whose views may not be in the mainstream, have complained that "behavioral advertising," as it is broadly defined in *The Principles*, somehow makes them uncomfortable.

---

<sup>6</sup> The State of Retailing Online 2007, Part 1 of 2

<sup>7</sup> Forrester Research, The State of Retailing Online 2007, Part 1 of 2.

We do believe that self-regulation and, in the case of retailing, industry leadership (or “leading practices”), are among the most effective ways to protect consumers while allowing businesses the flexibility to continue to innovate and adopt new technologies to better serve their customers. However, we were surprised to see the publication of; “*Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles*” (“*The Principles*”) by the Federal Trade Commission (“Commission” or “FTC”) at this time. While the Commission hosted a workshop on behavioral advertising in November 2007, it did not seem like the venue in which the FTC was building a complete record on this issue. Further, the Commission has not issued any follow-up findings or a report articulating specific consumer harms associated with broadly defined “behavioral advertising” practices. Finally, *The Principles* seem to sweep in a wide array of privacy issues that go well beyond simply moving forward a discussion about self-regulation of online advertising practices.

As a result, we would respectfully request that the Commission consider issuing a report on behavioral advertising outlining findings about consumer harms and the potential impact of the privacy concerns that have been raised. At this juncture, we think that while the FTC’s *Principles* have created a robust debate around the issue of behavioral targeting, they may be premature in that it is hard for any industry to formulate new “best practices” when the understanding of the perceived problem lacks clarity.

## **The definition of online “behavioral advertising” as set forth in *The Principles***

As the Commission staff has noted at recent in-person meetings, the definition of “behavioral advertising” was broadly drawn in order to generate the most amount of information about online advertising and marketing practices. That being said, we are very concerned that the definition not only encompasses third-party advertising practices, but first-party customer relationships as well. The proposed definition of “behavioral advertising” reads as follows: “the tracking of a consumer’s activities online 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.” As you know, retailers have engaged in extensive CRM (Customer Relationship Management) in both the catalog and brick and mortar world for years. As retailing moved online, CRM moved to the web as well, with first-party customer interaction being vitally important to both the retailer and to the consumer. However, the current definition makes no distinction between first-party and third-party interaction, and tracking that happens on a retailers’ proprietary website or family of websites (onsite), for example, as opposed to tracking that may occur on multiple unaffiliated sites across the web (network advertising).

As the *2007 SORO* report indicates, 55 percent of customers (both online and offline) have provided their e-mail addresses to retailers in order to receive marketing and promotional e-mail.<sup>8</sup> Many retailers also offer their customers the ability to create online accounts to speed checkout and respond to customer preferences. Account set-up allows customers to provide their name, physical address (for shipping, fraud prevention and catalog delivery), e-mail, phone number

---

<sup>8</sup> The State of Retailing Online 2007 Part 2 of 2.

and, if the customer chooses, credit card information. These types of accounts are most often username and password protected. With that information in hand, along with various other information gleaned about the customers purchases, browsing activity, and even abandoned shopping carts, retailers can further refine the shopping experience to appeal to that individual consumers' interests and needs, including delivering relevant marketing information onsite, via e-mail, or even in catalog form.<sup>9</sup> In fact, the most effective customer-facing interaction is powered by many different types of information collection.

As we have seen with the explosion of highly personalized sites such as Amazon.com and Netflix, consumers react very positively to personalized relationships with retailers. Again, all of this functionality is powered by *information collection* with the legitimate end-purpose of delivering relevant content to customers and improving the overall quality of web sites. As a result, we do not believe that what is, in essence, CRM should be swept up in the “behavioral advertising” debate. We also believe that our customers know what type of information is being collected on the site (from cookie placement to credit account management) and how that information it being used due to the fact that retailers' privacy policies are generally quite clear. Given the rapid growth of online retailing, we believe consumers have a

---

<sup>9</sup> For example: A customer will enter a retail site, browse for merchandise, add an item (in this case, shoes) to their shopping cart, and then “abandon” that cart, declining to complete the transaction. Retailers employ several strategies to convert cart abandonment to a completed sale. One popular method is to send a follow-up e-mail marketing promotion. In this scenario, the retailer recognizes the customer (through a previous cookie placement), knows that she has placed shoes in her shopping cart (again through cookie placement), and is able to deliver a message to that customer based on e-mail information that she has provided in the past. Often, these e-mails will contain an invitation to view other products on the site, offer a percent-off coupon, or a free shipping promotion. With the new information in hand, the customer is likely to return to the site, go back to her intact shopping cart (again made possible by cookie placement) and quickly purchase the shoes that she wanted.

very good comfort level with online interaction and benefit tremendously from this medium.

### **Transparency and Consumer Control**

Many retailers have painstakingly formulated online privacy policies that are very accessible and clearly and simply describe to customers how information (both non-identifying and PII) are being used on their sites, and when applicable, opt-outs are prominently noted. In fact, retailers have been industry leaders in communicating with consumers about privacy practices. Many privacy policies also include descriptions of technologies such as cookies and web beacons, describe how the sites are using them and remind consumers that they have the ability to set privacy preferences right on their own computer, such as disabling or deleting cookies (which also disables web beacons). Further, if third-parties are being used to collect information, deliver advertising, or send commercial e-mail, the consumer is generally advised of this and provided links to those vendors' websites where consumers can learn more and, if applicable, take advantage of informed options.

We fully support the notion of transparency (and the robustness of privacy policies across retail websites is a testament to that), and we also believe that ongoing consumer education about privacy options that are already available to them is essential. Consumers should be more informed about how to manage cookies in order to limit information collection and the placement of software on their computers. Consumers should also better understand they can *already* opt-out of marketing e-mails, telemarketing, certain marketing snail mail (such as prescreened offers of credit), and limit the sharing of sensitive financial information as under

FCRA and GLBA. It is also critical to note that these current opt-out regimes, as enacted by Congress, focus on information *use* and not on information *collection*. We very are concerned that the *Principles* have stepped into precarious territory when they suggest opt-out in the context of the collection of data. This is especially true for “behavioral” data that is most often non-identifying.

It is our belief that Principle One creates the potential for a “small-print web” where even common processes would have to be disclaimed by site operators. It is also hard to conceptualize a practical mechanism by which a consumer would exercise a real-time opt-out for cookie placement, the use of web beacons, or the collection of click-stream data for web site analytics, without significantly disrupting the feel and flow of retail sites. Would the retailer have to provide notice and opt-out before a marketing e-mail could be opened if that e-mail contained a web-beacon for marketing analytics that might later be used to deliver more marketing e-mail? Would the retailer have to provide an opt-out every time a customer placed something in their shopping cart and a cookie was simultaneously placed on their computer if that same cookie might be used to deliver promotional information the next time the customer visited the site? Would the same type of notice and opt-out have to be provided before a consumer could knowingly and voluntarily provide personally identifying information such e-mail, shipping and credit card information to complete a transaction?

While taken individually, these disruptions in the flow of the customer’s experience may not seem like a big deal to a lay person, but in terms of overall conversion rates these types of “hiccups” could be devastating. We all know how

frustrating pop-ups can be when you are simply trying to read the latest headlines on a newspaper website. Now transfer that experience to a retail website, where customers have come to expect a seamless experience from homepage to check-out. Even under the best circumstances, average conversion rates are only about 3.1 percent and shopping cart abandonment rates still hover at 50 percent.<sup>10</sup> Any additional hurdles would simply serve to frustrate consumers and drive down the number of completed transactions overall. Further, as the Commission knows from years of experience, even when offered the option, as required by law, consumers do not regularly take advantage of these types of programs. In fact, by our estimates, only 6 percent of retail customers exercised their right to opt-out of marketing e-mails in 2007<sup>11</sup>.

### **Reasonable Security and Limited Data Retention for Consumer Data**

We agree that reasonable security should be taken into account when safeguarding consumer information. While the GLB Safeguards Rule does not directly apply to the retail industry (unless being applied to sensitive financial information being held by retailers that are also financial institutions), we appreciate that the Commission regards the Safeguards Rule to be a model for good information security practices (as noted in both the DSW Shoe and B.J.'s Wholesale cases). That being said, the distinction should be drawn between security measures that are appropriate for PII or sensitive financial information and information that is generally more anonymous or non-sensitive such as general marketing data (e.g. name and address information).

---

<sup>10</sup> The State of Retailing Online 2007, Part 1 of 2.

<sup>11</sup> The State of Retailing Online, 2008.

The retail industry is also subject to a very complex private regulatory regime for safeguarding credit card information. As the Commission knows, retailers and the major card networks have been working on compliance with the Payment Cards Industry Standards (“PCI”) for several years, and several large retailers and the NRF sit on the PCI Security Standards Council. However, as we have seen with PCI, no security standard is ever going to be crime-proof. In fact, one of the most recent retail credit card security breaches happened to a grocery chain that was PCI complaint.

The business standard for the retention of customer data has generally been “as long as necessary to fulfill a legitimate business need.” We think that this standard has worked well, and has given different types of businesses the flexibility to determine what their own retention needs should be. Clearly reasonable retention periods may differ for sensitive information (such as full track card data) and less sensitive customer purchase information, for example. While the FTC staff has asked for comment on whether companies can and should reduce their retention periods further, we believe that this type of determination should be left up to private parties who review their own security standards and retention needs on an ongoing basis. Finally, we believe that anonymous information (such as click stream data) could be held indefinitely because it does not pose any inherent security risks.

### **Affirmative Express Consent for Material Changes to Existing Privacy Policies**

We were surprised to see the issue of affirmative consent (opt-in) for material changes to privacy policies surface in *The Principles*. While we are very familiar with

the FTC's July 2004, Gateway Learning / Hooked on Phonics settlement, we had, up until this point, viewed the Commission's determination in that case (to require opt-in on a going forward basis) to be punitive and specific to the facts in that case. As you know, privacy policies have been a matter of industry best-practices, and once a policy is adopted by a business it must follow the procedures set forth therein to avoid the appearance of being unfair or deceptive to consumers. That being said, different companies have developed many different mechanisms by which to notify their customers about changes in their policies, and, if they do provide customer choice in this area, many different mechanisms by which to provide that choice.

Requiring "opt-in," or affirmative consent, opens up a whole new set of challenges for retailers and consumers alike. First, in order to obtain an opt-in you must be able to effectively contact the customer. While it is easy to send a notice (as would be done in the opt-in context as well), it is quite another animal to insure that your customer actually opens the notice. E-mail "open" rates for retailers hovers in the 22 percent range<sup>12</sup>, and there are entire landfills full of "snail mail" privacy notices that are simply ripped in half and discarded before the customer even opens them. Even when the customer does read the correspondence, that consumer then has to affirmatively take action in an opt-in regime. Shop.org has tracked e-mail click through rates to be approximately 11 percent in 2006, with a conversion rate of 6 percent.<sup>13</sup> If these marketing statistics bear out in the context of opt-in, a retailer has an 88-94 percent chance that an opt-in could not be obtained every time a material change is made. That could be a devastating blow to marketing files.

---

<sup>12</sup> SORO 2007, Part 1 of 2

<sup>13</sup> Id.

Many retailers already affirmatively notify their customers of changes to their privacy policies or specifically request that consumers continue to check back to ascertain if changes have been made. Some even request an opt-out (as in the Gateway Learning case). Further, it would be a substantial departure from current national privacy standards to move to an opt-in regime as suggested in *The Principles*. The opt-in / opt-out debate has raged for years, and, as the Commission is aware, Congress has generally leaned towards *opt-out* when faced with issues of consumer choice -- and only for limited types of information sharing and marketing practices.<sup>14</sup>

**Affirmative Express Consent To (or Prohibition Against) Using Sensitive Data for Behavioral Advertising**

Principle Four, as proposed, states that; “companies should only collect sensitive data for behavioral advertising if they obtain affirmative express consent from the consumer to receive such advertising.” The Commission then asks for suggested “classes of information” to categorize as “sensitive.” At the November FTC forum discussion focused specifically on information that was used to market to children and to individuals with sensitive health conditions such as HIV-AIDS. However, these categories of information, as well as sensitive financial data, are already given significant protections under Federal law, while protections for other types of information have been much more ambiguous.

---

<sup>14</sup> E.g. GLBA, CAN-Spam, FCRA, FATCA, and the Telemarketing Sales Rule

It is our belief that the introduction of a potentially broad definition of “sensitive data” coupled with a new “opt-in” regime could create inequities in the marketplace. For example: specialty beer and wine purveyors can sell wine into many states over the internet -- would their customer’s behavioral information (related to purchasing alcohol) now be deemed “sensitive” under *The Principles* and subject to different rules than retailers selling expensive specialty cheeses? In fact, Principle Four creates a very a slippery slope when one considers all of the possible types of data that could potentially be covered and the competitive disadvantages that could be created. What about websites that sell vitamins or dietary supplements? Or websites that cater to specific religious or political groups? Or vacation sites that promote cruises to single, recently divorced or gay adults? All of this type of information could potentially be deemed “sensitive” under Principle Four, and require that operators of those sites be held to a different standard than operators of otherwise similarly situated sites. For these reasons, we believe that Congress has acted in the areas of highest concern (as discussed above) and that adding any areas should be carefully evaluated against existing legal and self-regulatory frameworks before potentially burdensome and inequitable new requirements are set forth.

### Conclusion

While we believe that *The Principles* have facilitated a healthy debate about marketing practices online as well as about consumer privacy in general, we believe that the publication of FTC-authored self-regulatory principles may be premature. As we mentioned above, it would be helpful for the Commission to issue a report outlining consumer harm and specified deficiencies in existing leading practices and

industry self-regulation. It is important to note that if the Commission issues final proposed “self-regulatory principles,” they likely will be viewed by the business community not as mere suggestions, but truly regulatory in nature, with perceived violations being considered “unfair and deceptive” under the FTC Act. With such an industry reaction, or overreaction, on the line, it is essential that a complete record be formed. We hope that the Commission approaches this area cautiously, knowing that legitimate online businesses, including retailers, really do strive to “do right” by their customers, and that online behavioral targeting should not be reactively vilified. At the end of the day, advertising and marketing have enabled the unprecedented growth of the web, and have made it an extremely attractive place for both retailers and consumers to do business.

Respectfully Submitted,

Elizabeth Oesterle  
Vice President, Government Relations Counsel  
The National Retail Federation

Scott Silverman  
Executive Director  
Shop.prg  
April 11, 2008