



June 4, 2010

The Honorable Rick Boucher
Chairman
Subcommittee on Communications,
Technology and the Internet
U.S. House of Representatives
Washington, DC 20515

The Honorable Cliff Stearns
Ranking Member
Subcommittee on Communications,
Technology and the Internet
U.S. House of Representatives
Washington, DC 20515

Dear Chairman Boucher and Ranking Member Stearns:

On behalf of the National Retail Federation (NRF) and Shop.org, we appreciate the opportunity to submit comments on the draft privacy legislation that you recently circulated. As you know, retailers are by their very nature marketers and advertisers. It is part and parcel of the industry, and trends and even revolutions, such as the rise of ecommerce, are fueled by the continuous sharing of information between merchants and their customers. The information collected ensures that stores are opened in locations where demand is the highest, the right merchandise is stocked on those shelves, and customers are offered the best sales and promotions to get them in the door.

Information gathering and the use of information by businesses has been widely demonized by groups that say that they represent consumers despite the clear benefits that the smart use of information has provided to retail customers. Indeed, privacy and security considerations are of paramount concern, but we believe that the draft goes too far in several key areas, and are concerned that it would have the unintended effect of stifling innovation and growth at a critical time for our economy. As you know, advances in information technology are notoriously rapid and consumers have come to expect retailers and other businesses to adapt to these changes and reflect these advances in their relationship.

As the world's largest retail trade association and the voice of retail worldwide, the **National Retail Federation's** global membership includes retailers of all sizes, formats and channels of distribution as well as chain restaurants and industry partners from the U.S. and more than 45 countries abroad. In the U.S., NRF represents the breadth and diversity of an industry with more than 1.6 million American companies that employ nearly 25 million workers and generated 2009 sales of \$2.3 trillion. 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 600 members include the 10 largest retailers in the U.S. and more than 60 percent of the Internet Retailer Top 100 E-Retailers.

Retailers have spent the better part of the last 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 both in-store and online. Ecommerce has brought millions of new customers to retailers' virtual stores and has also served to increase new customer traffic in brick and mortar shops as well. According to the Shop.org annual study, The State of Retailing Online ("SORO"), conducted each year by Forrester Research, Inc., online retail sales soared to \$156 billion in 2009 and it is likely that they will exceed the \$200 billion mark in 2012.¹

As retailers continue to fine-tune their selling and marketing strategies, consumers have, in particular, become more comfortable shopping online, especially with retailers that they know and trust. By the end of 2009, online sales accounted for 6 percent of all retail sales.² In contrast, it took the catalog industry 100 years to represent just 4.7 percent of retail sales.³ What has made this retail revolution possible is both the widespread access to the web and email by American consumers as well as 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 content and consumer-friendly store and 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 marketing and sales is the information that retailers have collected about their customers' shopping habits in stores and on their websites over time. That being said, retailers take their customer's privacy and security very seriously and have an excellent track record of using customer information in order to deliver relevant and targeted marketing. Retailers have long understood that keeping their customers happy is the most essential part of building positive long-term business relationships. However, retailers do not want to fundamentally alter an entire medium for effective information collection and delivery just because a limited number of parties have complained. 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. If businesses are not transparent about data collection and use, customers will not be happy and they will go elsewhere. In retail this is especially true, given the limitless number of choices presented to American consumers every day.

¹ The State of Retailing Online 2009

² The State of Retailing Online 2009

³ The State of Retailing Online 2002

The Draft Privacy Bill

Specifically, NRF is concerned that the proposed legislation lumps together under its definition of “covered information” many distinct types of information. SSN’s and financial account numbers are listed together with much less sensitive and widely available data such as name, address, and phone number. Additionally, non-personal identifiers such as Internet Protocol addresses, preference profiles, and cookies are, for the first time, also covered. Further, the definition of “sensitive information” includes categories such as race or ethnicity, religious beliefs, account information, and geolocation information, and subjects these data points to a strict opt-in regime. These are extremely broad and, in some cases, unprecedented definitions of covered information. These definitions could also put the bill in conflict with other information use statutes such as the Fair Credit Reporting Act and the Gramm-Leach-Bliley Act (GLB), as well as many state data breach statutes.

The first party opt-out requirement is also extremely troubling for retailers. 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. It is our belief that the current draft creates the potential for a “small-print web” where even common first-party processes would have to be disclaimed by site operators and customers would be constantly bombarded with marketing “choices.” We made these same points in our comments to the Federal Trade Commission (FTC) on their proposed self-regulatory principles, and the revised document contained a clear first-party exemption.

As the banking industry can attest, those yearly GLB notices that are required by law to be sent out to customers are routinely ignored without being opened. If consumers don’t even open their mail, it becomes hard to conceptualize a practical mechanism by which a consumer would have a privacy policy delivered and exercise a real-time opt-out without significantly disrupting their shopping session. Also, 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 “save the cart” for 30 days or deliver promotional information the next time the customer visited the site? Would the same type of notice 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” or consumer annoyances 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.⁴ Any additional hurdles would simply serve to frustrate consumers and could

⁴ The State of Retailing Online 2007, Part 1 of 2.

drive down the number of completed transactions overall. Further, we now know 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 2007⁵.

To further complicate matters, the draft bill would require notice and consent for the collection of offline information as well. This is fundamentally unworkable and raises many operational questions. Would a store clerk at point of sale be required to make sure a customer both received a privacy policy and understood the choices offered to them? Additionally, what new and expensive point of sale technology would be required to record a customer's choice if they opt-out? How would stores be required to keep track of that information when customers can shop in hundreds of store locations in several, if not all, states? Would Jane Smith in Oregon be recognized as the same Jane Smith who visited a store in Florida during a family vacation? And, if not, would a retailer be deemed in violation of the statute if information collection occurs if an opt-out was obtained across the country? With opt-out rates being historically low, would such investments even be worth the expense and employee training necessary?

The draft bill's requirement for opt-in for the sharing of covered information with unaffiliated third parties and opt-in for the collection or sharing of sensitive information is also very troubling. It would be a substantial departure from current national privacy standards to move to such a broad opt-in regime. The opt-in / opt-out debate has raged for years, and 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.⁶ It is also important to mention again that consumers do not traditionally exercise choice -- they rarely opt-in and they rarely opt-out. The effect of this provision is compounded again by the overly broad definitions of "covered information" and "sensitive information." To require opt-in for many activities like transferring customer information for third party data analytics, using customer emails to link to a retailer's Facebook page, asking customers about their pregnancy to market maternity clothes or baby gear, or even deploying cutting-edge mobile marketing technologies will simply make these tasks impractically difficult. Current requirements subject only the most sensitive data to opt-in, and generally only require opt-out for marketing purposes. We do not believe the intent of the draft was to go this far, and urge you to reexamine the current standards employed in other privacy-related statutes.

We were also surprised to see the issue of affirmative consent (opt-in) for material changes to privacy policies in the draft bill. While we are very familiar with the FTC's July 2004 Gateway Learning / Hooked on Phonics settlement, the Commission's determination in that case (to require opt-in on a going forward basis) was punitive and specific to the facts in that case which involved information about children. 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

⁵ The State of Retailing Online, 2008.

⁶ E.g. GLBA, CAN-Spam, FCRA, FATCA, and the Telemarketing Sales Rule

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 range⁷, 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.⁸ 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 would be an additional debilitating blow to marketing files.

We live in the “information age” and we also live in a consumer driven economy where two-thirds of GDP is directly attributable to consumer spending. Stifling information flows and innovations in technology (such as mobile marketing, for instance), would have a very detrimental effect on already sluggish retail sales. We are very concerned that the draft bill goes too far by eliminating the traditional first-party marketing “exemption,” as well as creating new classes of protected information, and moving too swiftly towards an opt-in regime. We appreciate the opportunity to comment on the draft bill and hope to work with you in the coming months to further refine the bill’s scope.

Sincerely,



Steve Pfister
Senior Vice President
Government Relations
National Retail Federation



Scott Silverman
Executive Director
Shop.org

⁷ SORO 2007, Part 1 of 2

⁸ Id.