Walmart
Save money. Live better.

702 SW 8th Street
Bentonville, AR 72716
Phone 123.456.7890
Fax 123.456.7892
www.walmart.com

June 14, 2010

National Telecommunications Administration
US Department of Commerce
Room 4725
1401 Constitution Avenue NW
Washington, D.C. 20230

Re: Docket No. 100402174-0175-01

Wal-mart Stores Inc. (Walmart) appreciates the opportunity to respond to the Department of Commerce National Telecommunications and Information Administration's Notice of Inquiry (NOI), "Information Privacy and Innovation in the Internet Economy." Walmart thanks the Department for examining this important issue.

In order to provide context, we first describe Walmart's engagement in this area. We then break our remarks into the following topics:

- The value of a principles-based approach to privacy;
- Key privacy principles and the continued value of notice and choice;
- Other relevant principles and comments on a use-based approach; and
- Jurisdictional and enforcement issues.

Walmart's Role and Privacy Perspective

As the largest retailer and private employer in the U.S., with approximately 1.4 million employees and 140 million customers coming through U.S. stores every week, Walmart considers an array of privacy issues on a daily basis. Walmart approaches privacy from a very broad perspective. Walmart operations cover almost every conceivable privacy topic, channel, and geographical region. Walmart operations include:

- Operating as a "brick and mortar" retailer, with over 3500 outlets domestically.
- Operating as a leading online merchant through walmart.com. According to Hitwise, a service that measures online usage, Walmart.com is among the top five most visited ecommerce websites in 2009.

- Operating over 600 Sam's Clubs domestically, which offer a membership model for its customers.
- Conducting extensive global retail operations throughout the world, including Europe, Canada, Asia, and Central and South America.
- Communicating with our customers across multiple channels, e.g. via email, postal mail, mobile devices, websites, and our stores.
- Collecting and merging data through numerous sources, including customers themselves, third party sources, and technology such as websites.
- Providing a wide variety of products and services. Some of these are more regulated regarding privacy or personal data than others. Examples include health services (some of which are covered by HIPAA and some of which are not like personal health records); financial products and services governed by the Gramm-Leach-Bliley Act; sales of hunting and fishing licenses; and sales of over-the-counter products containing pseudoephedrine.
- Serving in a leadership role in technology, online or offline. Some of these technologies have privacy implications, including online advertising, Radio Frequency Identification (RFID), or mobile devices.

In sum, Walmart has a deep engagement with consumers in a variety of contexts. We have made it our business to understand what customers want. Consequently, we respectfully submit that Walmart has a strong understanding of not only the dynamics of compliance with myriad privacy requirements, but also what we see as the underlying goals of what privacy rules seek to accomplish for consumers.

Principles-Based Approach

As an initial matter, we note that the scope of the NOI focuses on the Internet, although many questions in the NOI have a wider application. We welcome this wider scope. Since the emergence of online behavioral advertising as a topic of legislative and regulatory interest, we have been concerned that policymakers evaluating privacy issues may narrow their focus to the practices and concerns relating to Internet practices. This can lead to less upfront involvement of other sectors that face similar privacy issues. However, inevitably, and correctly, other practices become part of the debate. It does not serve consumers or businesses well when these issues are bolted on late or later in the process. This can lead to inconsistent or skewed regulatory schemes that may fit poorly or be ineffective. For the vast majority of U.S. businesses, this could be cumbersome at best and unworkable at worst, and also likely will not address the underlying issues for consumers. It is thus imperative that, as privacy frameworks are developed, policy-makers take the time to

understand the impact to consumers and companies that have online as well as offline relationships.

In considering how to examine privacy effectively, Walmart favors a principles-based approach. We think this is the best way for privacy to work for companies and consumers. It also provides the right foundation to discuss global privacy issues with stakeholders in other countries. Having a set of framework principles in place that can be applied in many different contexts would provide an effective, consistent approach to privacy. A privacy regime based on a well-conceived set of principles could be applied to every new technology, every new marketing channel, and every new use of consumer information. Such a framework would impose coherent and predictable standards that are easily understood by both consumers and businesses. We believe that the more coherent the guidance, the better the customer communications and business compliance will be.

A principles-based approach to privacy is certainly not new. Indeed, it is how existing models are framed, including the FTC's Fair Information Practice Principles, the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, and the APEC Privacy Framework. Focusing on core privacy principles would facilitate the creation of predictable standards, and help avoid repeatedly dedicating time and energy to the creation of ad hoc requirements to address emerging technologies or business activities. While it may be possible to devise customized requirements to address privacy issues on an individualized, technology-specific basis, we question the efficiency – and, more importantly, the outcome – of such an approach. Not only does it create difficulties for companies attempting to develop an overarching approach to privacy, it also puts consumers in the position of having to navigate a confusing maze of unpredictable standards.

As an example of a principle-based approach, last summer we updated our customer privacy policy for Walmart domestic operations. The updated policy is based on the Fair Information Practice Principles and developing industry standards and global guidelines. Our goal was to make the policy transparent, to meet best practices, and to be integrated across all business units and product offerings. This initiative gave us further insights into how to focus on underlying privacy principles and then to operationalize them.

Key Privacy Principles

We believe certain core principles round out a privacy framework. One way to think about privacy principles is from the consumer's point of view. There appears to be four distinct principles that inherently involve direct interaction between a consumer and a business. These principles are notice, choice, access/correction, and accountability. Other

privacy principles typically involve internal data practices. Each of these principles is discussed below.

Consumer Notice and Choice

As part of a principles-based approach, we would like to turn to the key aspects of notice and choice that were raised in the NOI. We understand that a growing topic in the public policy debate is whether a traditional privacy approach, including consumer notice and choice, is still valid as technology, business practices, and consumer expectations evolve. We do believe that notice and choice still have a central place. This is not to say that there are no other protections to consider as a framework is developed. But we should not lose sight of a key way that consumers interact with businesses. We believe that notice and choice are key elements of a principles-based approach that need to be flexibly applied among various technologies and to meet consumer needs. We offer the following examples to show the value of notice and choice.

As one example, Walmart has begun pilot programs with mobile messaging. These messages can alert customers that pharmacy prescriptions are ready for pick-up, or about special offers in a store. Notice and choice are essential to make mobile interactions work. Indeed, direct marketing efforts, and the laws and industry practices that bound them, operate on a notice and choice model. We are not aware of another model that could work well for direct marketing.

Another example concerns our experiences with the use of Electronic Product Code (EPC) technology. At the simplest level, EPC is the next generation bar code. Currently, EPC is primarily used to track certain case and pallets in the supply chain. When EPC may be offered on individual products on the sales floor, future potential consumer benefits are real and direct. Examples include receipt-less returns; product authenticity and traceability; and food and product safety. Even though EPC tags used in retail contain no personal data, we are building in privacy protections.[1] As a cornerstone of EPC development, Walmart is

[1] Walmart also follows industry standards and policy-maker guidance with regard to its EPC usage. Walmart follows the Guidelines on EPC for Consumer Products issued by GS1 EPCglobal, the standard-setting body for EPC, in 2003 with final adoption in 2005. We also adhere to the EU Commission Recommendation published in May 2009 regarding the implementation of privacy and data protection principles for applications supported by radio-frequency identification. This includes use of a Privacy Impact Assessment (PIA) tool.

designing its use to enable choice. The goal is to provide EPC tags that are readily removable from the product or packaging, such as by placement on the price tag, or that can be deactivated if embedded for those who are concerned. We believe that choice is the right model for this technology. Some, perhaps most, consumers will appreciate its benefits. Some will not. But ultimately consumers should be able to choose which they prefer.

There are certainly challenges to notice and choice. For notice, it can be difficult to establish when to provide it and what is the right content. We should be careful to avoid prescribing notice with only certain channels in mind. For example, notice requirements that essentially require serving a pop-up on a website, or that require a template based on mail notices, may not work in other environments. The more specific the requirement, the less likely it will work in different contexts or technologies, and the strictures may also not serve the intended purpose. As another example, in terms of timing, it may only be feasible to provide notice close in time but not before data collection (think of security cameras in stores). Perhaps a better terminology is openness. This would demonstrate a company's commitment to providing basic and also complete information about data practices. It could encompass such items as immediate notice, layered notice, and also availability of the full policy based on a consumer's interest. Effective notice should cover both how consumers will know technology or certain business activities are in operation – and also how they can understand what the technologies or practices mean. Fundamentally, however, consumers should have access to information about business practices.

Regarding choice, the most basic challenge is being clear about when choice should apply. Clearly choice is appropriate for direct marketing. In our discussion of EPC, we have also provided an example related to removing or disabling a technology. But in what other circumstances should choice apply – e.g. data sharing, social media, geolocation – and what is the underlying principle? Unless choice is to be removed from a privacy framework – which seems unlikely given its centrality to direct marketing and customer relations – there must be clarity about when it applies. Otherwise there will be a murky standard that will be hard to explain and offer to customers and harder to implement.

Other Principles and a Use-Based Approach

In addition to notice and choice, other privacy principles include access/correction, accountability, and data management. As we understand and apply an access principle, consumers should be able to find out what information companies maintain about them, and request correction of the information. If the access requests are administratively burdensome, and involve non-sensitive data, the company should be able to respond by describing the types of data it typically maintains. If a consumer requests corrections,

companies should make the changes or explain to the consumer why a correction could not be made. Companies can impose reasonable authentication and other mechanisms to support access and correction requests.

Companies also should be accountable for compliance with privacy principles. Besides internal governance structures, accountability also includes how companies offer consumers a redress mechanism for their questions or concerns. Retailers deal with consumer questions and requests on a daily basis and have been doing so for years. It is part of the business-consumer relationship to respond to consumer wants and needs. We make it a priority to respond fully and timely to the customer inquiries we receive about privacy.

Other privacy principles tend to relate to internal data management. These principles could be encompassed under an umbrella principle related to information management or responsible uses. As examples, these include data integrity, security, disposition, and data uses. We agree that terminology relating to primary and secondary purposes has outlived its usefulness, and in fact probably never reflected business realities. The fact is that information is often collected for multiple purposes or uses. Certain groups, like the Centre for Information Policy and the Business Forum for Consumer Privacy, have done excellent work examining and describing common legitimate business purposes. This work is especially helpful as policy-makers consider how to frame principles across different business models. For instance, notice and choice may be more relevant for companies with direct B-C relationships, whereas a used-based model may be more effective for companies e.g. that perform data brokerage activities.

We offer a couple of caveats regarding a use-based framework. First, as discussed above, careful consideration needs to be given to how to incorporate notice and choice principles. Second, how to implement a use-based model needs consideration. We sometimes hear the FCRA raised as a workable model for used-based principles. The FCRA may well be a good model for sensitive data that is used for high impact activities like offers of credit or employment. However, we question whether that sort of model is appropriate for non-sensitive contact information used for lower impact activities like data analytics or marketing. It may well set up a large compliance burden and costs that produce little or no value for consumers. Rather, a use-based model should set forth appropriate criteria to which companies can adhere without unnecessary complexity.

Jurisdiction and Enforcement

The Department raises a number of questions about the impact of privacy rules being set by a number of different jurisdictions – state, federal, global – and how they can be broad-based or sectoral. We believe that a framework that is principles-based can do a great

deal to harmonize these different rules. We may find that the differences are not as great as first believed. We do believe federal standards are more appropriate, especially in interstate commerce areas like website operations, and also enable clearer conversations with our global partners.

As policy-makers work through jurisdictional issues, we wish to draw attention to two areas. First, careful consideration needs to be given to accommodating existing laws, especially sectoral laws. It would be simpler, and certainly convenient, to provide that a framework sits on top of and does not impact these laws. However, this is easier said than done. It could lead to different and perhaps conflicting requirements applying to the same data, which would be problematic for business and consumers.

Second, consideration should be given to the best methods to enforce a privacy framework. A common recent trend, at least in part, is to propose FTC and state AG enforcement. We think that can be a workable model. However, an area of concern is potential penalties. One advantage to a principles-based approach is it allows policy-makers to focus on the outcomes or impacts that are important to consumers—this helps set the framework. Another advantage is that, as it provides insights into the outcomes or impacts to avoid or minimize, this should also help guide enforcement parameters. We think it may be inappropriate to apply a simple formula of a dollar penalty per violation in all circumstances. Such a regime may make sense, for instance, in a direct marketing situation, where illegal conduct directly touches consumers and the sanction serves to penalize improper profit. However, if a framework is intended to cover the broad range of privacy issues, like responsible data management and disposal, we wonder if this formula makes sense in all contexts. As an example, if paper is not properly shredded before it is recycled, or if access controls are not properly implemented initially, there may be a violation of company procedures but with low or minimal impact if corrected. A per violation penalty is hard to envision – how do you measure each violation – and appears to impose strict liability unrelated to consequence. Just like with other aspects of a privacy framework, enforcement and penalties need careful consideration as well.

Conclusion

The Department's final question is how can it help address issues raised in the NOI. We believe that the Department can help by continuing this effort and remaining engaged in the privacy debate. This will help the U.S. framework as well as the dialogue within the global community. Walmart welcomes the Department's participation. Please feel free to contact Zoe Strickland, Vice-President, Chief Privacy Officer, at zoe.strickland@wal-mart.com with any questions or comments.