Before the
Department of Commerce
National Telecommunications and Information Administration

In the Matter of	)	
Multistakeholder Process to Develop Consumer Data Privacy Codes of Conduct	)	Docket No. 120214135-2135-01

COMMENTS OF LIFELOCK

Clarissa Cerda
Senior Vice President, General Counsel & Secretary
LifeLock, Inc.
60 E. Rio Salado Parkway, Suite 400
Tempe, AZ 85281

April 2, 2012

LifeLock, Inc. ("LifeLock") appreciates the opportunity to respond to the National Telecommunications and Information Administration ("NTIA") request for comments on the proposed "Multistakeholder Process to Develop Consumer Data Privacy Codes." Specifically, NTIA seeks comments on which consumer data privacy issues should be the focus of NTIA-convened multistakeholder processes and specific procedural considerations that NTIA should take into account when initiating a privacy multistakeholder process.

LifeLock focuses its comments on a fundamental consumer privacy issue that should be a focus of the first NTIA-convened multistakeholder processes – transparency. As the FTC Privacy Report underscores, there is a pressing need to ensure that consumers receive easily understandable and accessible information about privacy and security practices. LifeLock suggests a two-phased approach to provide consumers with transparent privacy policies. First, is development of a simple, standardized, transparent rating system that uses colors and numbers to indicate the exposure level associated with data collection practices. Second, is industry coordination on standardized and clear privacy policies that enable consumers to understand data collection and use practices.

I. About LifeLock

LifeLock provides a wide range of privacy protection services to consumers, including identity theft protection and data breach response services. Headquartered in Arizona, LifeLock's agents and identity theft resolution specialists help our members keep their identities safe 24 hours a day. We have a strong focus on educating consumers

and working with policymakers to better understand the increasing threats of identity theft. For example, LifeLock proactively combats identity theft through a partnership with the nonprofit FBI Law Enforcement Executive Development Association ("FBI-LEEDA".) Working with FBI-LEEDA, LifeLock hosts summits open only to elected officials and law enforcement. The one and two-day events, attended by chiefs, sheriffs, investigative supervisors and fraud unit investigators, address a range of identity theft issues, including laws, new technologies, and investigative techniques to assist in identity theft investigations and victim's assistance.

Through this work, LifeLock has a sophisticated understanding of identity theft and how the crime causes severe disruptions to Americans' lives. As such, we applaud the Executive Office of the President ("EOP") for making identity theft not only a focus of the blueprint, but also a focus of the Administration. With as much as $15 billion lost annually to identity theft, the crime not only is life-disputing to victims but threatens to undermine the nation's very financial stability.[1] As the dominant consumer fraud complaint, about 8.1 million Americans were reportedly victims of identity fraud in 2010, and the average identity fraud victim incurred a mean of $631 in costs as a result of the fraud—the highest level since 2007.[2]

[1] FTC Identity Theft Survey Report (2007), *available at* http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf.

[2] Federal Trade Commission, Consumer Sentinel Network Data Book for January–December, 2010, March, 2011, *available* at http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2010.pdf.

II. The Proposal: Rating System and Standardization of Privacy Notices

NTIA requests comments on which consumer data privacy issues should be the focus of the initial multistakeholder processes. LifeLock agrees with NTIA's suggestion that mobile privacy notice would be a valuable first topic. Indeed, the FTC's Final Privacy Report, "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers," notes "the urgency for the companies providing mobile services to come together and develop standard notices, icons, and other means that the range of businesses can use to communicate with consumers in a consistent and clear way. *Id.* at 64.

LifeLock suggests that the working group address both icons and standardized notices. One working group track would develop a simple, standardized, transparent rating system for consumer privacy notices that can be implemented quickly in icon format. The second track would standardize privacy notice elements. We believe this approach would expeditiously address the transparency and consumer empowerment interests without chilling innovation or beneficial uses of consumer information.

A. Phase One: Color/Number Coded Icon/Seal System

As the Administration White Paper accurately observes, the current framework has led to long, complex, and incomprehensible privacy policies that consumers cannot understand. At the very point where consumers could gain a meaningful understanding of privacy risks, companies all too often provide unclear descriptions of what personal data they collect, why they need the data and how they will use it. For this reason, we believe that consumer privacy notices should clearly and in a standardized manner

indicate the extent to which consumer information may be collected, used, and disclosed when a consumer provides data to a commercial, non-profit, or governmental entity.

We propose a standardized, color-coded and numbered privacy seal or icon system that would make immediately apparent to consumers whether their data may be transferred to a database of information used to compile individual profiles. For maximum effectiveness, the privacy seal or icon should be prominently featured on the home page of the website and near the request for information and would disclose data practices as follows:

1. A clear and conspicuous green seal or icon featuring the number "1" would indicate that a commercial, non-profit, or governmental entity does not disclose consumer data or does so only for the referenced "commonly accepted" internal practices required to process the consumer data;
2. A clear and conspicuous yellow seal or icon with the number "2" would indicate that a commercial, non-profit, or governmental entity discloses information in ways that require consumer choice but that does not lead to proliferation of consumer data, or that discloses information in a format that cannot reasonably be re-identified; and
3. A clear and conspicuous red seal or icon containing the number "3" would indicate that a commercial, non-profit, or governmental entity sells, exchanges, or publicly discloses consumer information or discloses that information to any other external entity, such as a data broker, that in turn offers it for sale, exchange, or public disclosure, containing a standardized, concise statement in the icon about the disclosure.

It is particularly important that this third, higher risk category be reserved for practices that proliferate consumer information in ways that can readily identify individuals. Such practices are qualitatively different from the practices described in the first and second, lower risk categories as such practices build large consumer profiles and are rarely transparent to consumers under conventional privacy notices.

In addition, because the practices described in the third category are higher risk and have raised more concern regarding consumer transparency and choice, an opt-out option should be offered in connection with these activities. Conversely, the practices described in the first and second categories are much lower risk and are respectively transparent to consumers. Thus, the practices described in the first and second categories would not, at this time, need an opt-out option.

Each icon would contain a link to a concise and specific explanation of the significance of the color/number code. This system should apply equally to non-profits and governmental entities, where they disclose consumer data. This proposed notice system has the major advantages of: (a) being immediately visible to consumers; (b) being easy for both consumers and commercial, non-profit, or governmental entities of all sizes to understand and apply, thereby promoting competition and consistency in privacy practices; (c) being deployable on paper, mobile, and web media without the need to build and agree on technical standards or interfaces; (d) providing transparency regarding data collectors' relationships with non-consumer facing entities that compile consumer profiles; (e) avoiding preempting site-by-site consumer choice, as well as imposition of a technology mandate; and (f) fitting well with existing seal programs, while covering both behavioral advertising and other data sharing models.

B. Phase Two: Standardized Privacy Bullet Points

The second track of this transparency solution would offer standardized and easily understood points that would appear when, in an electronic format, the user clicked on the icon or seal. We recommend standardized bullets describing consumer data practices, rather than longer, standardized privacy notices because the standardization of privacy notices is far too complex and difficult to achieve in a short period of time and can serve to mask the associated risks. Rather, we recommend creating a directory of data collections, uses, and disclosures that correspond to standardized bullet points.

Under this approach, when users click on the icon or seal, they would go to a "Privacy Notice" page. However, instead of seeing a common, overly legalistic privacy notice, they would see a list of standardized bullets – easier to understand, more transparent, easier to normalize – that would eliminate legalese and use plain English so as to effectively and efficiently provide consumers with information regarding data collection, use, and disclosure.

We emphasize the critical role of consumer transparency as the first step to consumer control. This rating/seal system could evolve to include additional opt-out options as self- regulation evolves. However, this basic system addresses consumer transparency and sets the foundation for basic consumer control through informed decision-making while at the same time facilitates greater consumer control later as opt-out technologies are perfected.

III. Implementation and Enforcement

The proposal described above would be self-executing – each company/advertiser making a designation decision would make that decision based on the Code of Conduct. That designation would then be considered a material statement to consumers that would be actionable under Section 5 by the Federal Trade Commission as an unfair or deceptive business practice if the applicable entity failed to live up to the designation.

We thank you for considering our views, and are eager to continue to work with you in a constructive fashion to help achieve NTIA's goals of balancing consumer transparency and choice with beneficial uses of information and continued technological innovation.

Respectfully submitted,

_____

Clarissa Cerda
Senior Vice President, General Counsel & Secretary
LifeLock, Inc.
60 E. Rio Salado Parkway, Suite 400
Tempe, AZ 85281