

**Before the
U.S. Department of Commerce**

)	
)	
In the Matter of the Request for)	
Comments on the Department of)	
Commerce’s Report Entitled “Commercial)	Docket No. 01214614–0614–01
Data Privacy and Innovation in the Internet)	
Economy: A Dynamic Policy Framework”)	
)	
)	
)	

COMMENTS

OF

LIFELOCK, INC.

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

January 27, 2011

January 27, 2011

FILED ELECTRONICALLY

**National Telecommunications and Information Administration
US Department of Commerce**

**In the Matter of the Request for Comments on
Department of Commerce's Report Commerce's Report
Entitled "Commercial Data Privacy and Innovation in the
Internet Economy: A Dynamic Policy Framework."
Docket No. 01214614-0614-01**

Comments of LifeLock, Inc.

LifeLock, Inc. ("LifeLock") appreciates the opportunity to respond to the U.S. Department of Commerce Internet Policy Task Force's "Green Paper" on privacy: "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework" ("Green Paper"). LifeLock commends the Department of Commerce ("Department") on its efforts to update the current privacy framework to meet the privacy challenges of the twenty-first century while supporting beneficial uses of information and technological innovation.

We strongly support the Green Paper's observations regarding the need for improved transparency for consumers regarding online data collection and sharing. Indeed, both "Do Not Track" and "Why Did I See This Ad" self-regulation and Internet cookie control mechanisms are in place today but have seen little adoption or utilization to date. We believe this is due to lack of understanding by consumers of the types of information captured and the fact that the information is held in profiles by third parties with whom the customer has no relationship. Because of this lack of understanding, consumers need to be provided with clearer indications when their information is being captured and provided for profiles held by data brokers or made publicly available.

In particular, we respond to the Green Paper's request for comments on the best approach to improve transparency and enhance consumer choice in an era when consumer data flows far more widely than consumers presently understand.

In brief, we propose a two-phased approach that promotes transparency and establishes baseline privacy principles. First, we promote a simple, standardized, transparent rating system that uses colors/numbers to indicate the risk level associated with data collection and use practices. Such a system can be implemented quickly to provide notice to consumers. Second, we urge standardized privacy notice elements developed with industry input. These notice elements would be standardized bullet points that explain data collection and use practices in a clear and effective manner.

I. About LifeLock

LifeLock provides a wide range of services to consumers with respect to privacy protection, including identity theft protection and data breach response services. Headquartered in Arizona, LifeLock's 300 agents help our members keep their identities safe 24 hours a day. The company has a strong focus on educating consumers and working with law enforcement and elected officials to better understand the increasing threats of identity theft. LifeLock was recently ranked 8th on Inc. magazine's 29th Annual Inc. 500 List, a ranking of the nation's fastest-growing private companies.¹ In addition, LifeLock was recognized as #1 in the Security category.² LifeLock does not transfer consumer data but has thought extensively about transparency issues raised in this proceeding.

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

The Department requested comments on the best approach to promote transparency so that consumers can make informed choices in an information economy. LifeLock urges a two-phased approach that promotes transparency and establishes baseline privacy principles, which is easy for consumers to understand and thus allows consumers to make informed decisions. First, we promote a simple, standardized, transparent rating system for consumer privacy notices that can be implemented quickly. Second, we urge standardized privacy notice elements developed with industry input. We believe this approach would expeditiously address the transparency and consumer empowerment interests that animate the Green Paper, without chilling innovation or beneficial uses of consumer information.

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

As the Department accurately points out, the current framework has led to long, complex, and incomprehensible privacy policies that consumers cannot understand.³ 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

¹ See <http://www.inc.com/inc5000/list/industry/security>.

² See <http://www.inc.com/inc5000/list/industry/security>.

³ See Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework (Dec. 16, 2010) at Section II.B.

does so only for what the Federal Trade Commission’s Staff Report⁴ calls “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.

⁴ Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers (Dec. 1, 2010).

B. *Phase Two: Standardized Privacy Bullet Points*

The second phase 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. This approach is much easier than standardizing privacy notices, and the bullets can be based on the Department's suggested purpose specifications and use limitations.

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.

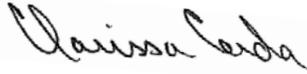
We emphasize the critical role of consumer transparency as the first step to consumer control. This rating/seal system could evolve to include additional opt-out options as self-regulation evolves. However, this basic system addresses consumer transparency and sets the foundation for basic consumer control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

C. *Implementation and Enforcement*

The proposal described above would be self-executing – each company/advertiser making a designation decision would make that decision based on criteria, though not regulations, enunciated by the Federal Trade Commission and/or Department of Commerce with industry input. 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. Self-regulatory organizations would refer non-compliance to the Federal Trade Commission for investigation and/or enforcement, just as the Better Business Bureau's NAD has long referred deceptive advertising cases to the Federal Trade Commission for enforcement.

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

Sincerely,

A handwritten signature in black ink that reads "Clarissa Cerda". The signature is written in a cursive style with a large initial 'C'.

Clarissa Cerda
Senior Vice President, General Counsel & Secretary