Improving Transparency and Enhancing Choice: A Proposed Rating and Privacy Notice Method to Alert Consumers to Company Data Collection and Use Policies

By Clarissa Cerda

I. Introduction

This paper examines a new method 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. This approach is based on the need for improved transparency for consumers regarding online data collection and sharing. Indeed, while both "Do Not Track" and "Why Did I See This Ad" self-regulation and Internet cookie control mechanisms are being deployed today, they have seen relatively little consumer utilization to date. It is likely that this is due to consumers' lack of understanding by of the types of information captured and the fact that the information may be held by third parties with whom the customer has no relationship. To address this lack of understanding, consumers should be provided with clearer indications when their information is being captured and passed along to data brokers or otherwise made publicly available.

This paper focuses on the central challenge of improving transparency and enhancing consumer choice in an era when consumer data flows far more widely than consumers presently may understand. This paper proposes a two-phased approach that promotes transparency and establishes a baseline privacy principle.

First, this paper proposes the development of a simple, standardized, transparent rating system that uses colors/numbers to indicate the exposure level associated with data practices. Such a system can be implemented quickly to provide notice to consumers. It is also ideal for notice over mobile handsets, the likely topic of the National Telecommunications and Information Administration's (NTIA's) first multi-stakeholder privacy negotiation to implement the White House Privacy White Paper[1] report setting out a proposed policy framework for US consumer privacy.

Second, this paper proposes the implementation of 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.

[1] 77 Fed. Reg. at 13098, 13099 (Mar. 5, 2012).

II. The Historical Landscape

To date, the US Government's efforts, through the Federal Trade Commission (FTC), have balanced the privacy interests of consumers with the need to encourage industry innovation. The lynchpin of that approach has been transparency. As FTC Chairman Leibowitz explained, "…the FTC wants to help ensure that the growing, changing, thriving information marketplace is built on a framework that promotes privacy, transparency, business innovation and consumer choice."[2] Similarly, transparency is a core feature of the proposed privacy framework in the "Privacy Bill of Rights" set forth in the White House Privacy White Paper.[3] This paper proposes a privacy notice framework that is designed to realize that concept. The proposed approach is fully consistent with the FTC's many efforts over the past decade and in recent years to drive transparency and consumer control.

A. FTC Rules Aimed at Promoting Clarity in Consumer Disclosures

The FTC has brought a long series of enforcement actions against companies that made material misrepresentations about their privacy policies with regard to personal identifiable information,[4] culminating in its Sears, Roebuck & Company consent decree in July 2009.

The approach proposed here is consistent with the FTC's settlement in Sears, Roebuck & Company, which made clear that it is a deceptive practice to bury notice of intrusive data collection practices in a long end-user license agreement (EULA), even if the consumer opts-in and is compensated for accepting the contract.[5]

---

[2] Press Release, Federal Trade Commission, FTC Staff Issues Privacy Report, Offers Framework for Consumers, Businesses, and Policymakers (Dec. 1, 2010).

[3] Consumer Privacy in a Networked World, A Framework for Protecting Privacy and Promoting Innovation in the Digital Economy, at 14-15 (Feb. 23, 2012).

[4] *See, e.g., FTC v. Toysmart.com, LLC*, No. 00-11341-RGS, 2000 WL 34016434 (D. Mass. July 21, 2000); *In re Liberty Fin. Cos.*, 128 F.T.C. 240 (1999); *FTC v. ReverseAuction.com Inc.*, No. 00-0032 (D.D.C. Jan. 6, 2000); *FTC v. Sandra Rennert*, No. CV-S-00-0861-JBR (D. Nev. July 6, 2000); *In re Premier Capital Lending, Inc.*, No. C- 4241, 2008 WL 5266769 (F.T.C. Dec. 10, 2008); *In re Life Is Good, Inc.*, No. C-4218, 2008 WL 1839971 (F.T.C. Apr. 16, 2008); *In re Petco Animal Supplies, Inc.*, 139 F.T.C. 102 (2005); *MTS, Inc.*, 137 F.T.C. 444 (2004); *In re Microsoft Corp.*, 134 F.T.C. 709 (2002); *In re TJX Cos.*, No. C-4227, 2008 WL 3150421 (F.T.C. July 29, 2008); *In re Guidance Software, Inc.*, No. C-4187, 2007 WL 1183340 (F.T.C. Mar. 30, 2007); *In re Petco Animal Supplies, Inc.*, 139 F.T.C. 102 (2005); *In re Guess?, Inc.*, 136 F.T.C. 507 (2003); *FTC v. Navone*, No. 2:08-CV-001842 (D. Nev. Dec. 30, 2008); *United States v. Am. United Mortg. Co.*, No. 1:07-CV-07064 (N.D. Ill. Dec. 18, 2007); *In re CVS Caremark Corp.*, No. C-4259, 2009 WL 1892185 (F.T.C. June 18, 2009); *United States v. Rental Research Serv.*, No. 09 CV 524 (D. Minn. Mar. 5, 2009); *United States v. ChoicePoint, Inc.*, No. 1:06-CV-0198 (N.D. Ga. Feb. 15, 2006).

[5] *In the Matter of Sears Holdings Management Corp.*, Complaint, Docket no. C-4264 (Aug. 31, 2009).

The consent order in that case requires Sears to "[c]learly and prominently, and prior to the display of, and on a separate screen from, any final 'end user license agreement,' 'privacy policy,' 'terms of use' page, or similar document, [to] disclose all types of data that would be the subject of any tracking application, how such data may be used, and whether the data may be used by a third party."[6]

At an FTC Privacy Roundtable on December 7, 2009, Chairman Leibowitz characterized the essential deceptive practice to be:

> *… while the extent of tracking was described in the EULA, that disclosure wasn't sufficiently clear or prominent given the extent of the information tracked, which included online bank statements, drug prescription records, video rental records, library borrowing histories, and the sender, recipient, subject, and size for web-based e-mails. So, consumers didn't consent with an adequate understanding of the deal they were making.*[7]

Notably, the framework proposed here would achieve the FTC's central goal of providing clear and prominent notice of information collection, use, and disclosure practices.

B. Online Behavioral Advertising

Similarly, the FTC's February, 2009 Staff Report on online behavioral advertising[8] ,as part of the principle of transparency and consumer control, embraced the requirement of a clear, prominent, consumer-friendly disclosure that data are being collected to provide tailored advertising so that consumers could choose whether to have their information collected for that purpose.[9]

One approach the FTC Staff Report discussed was of a method for to notifying consumers of the websites' online behavioral advertising practices, which is very similar to this paper's proposal. This is the "Why did I get this ad?" disclosure located in close proximity to an advertisement that links to the pertinent section of a privacy policy explaining how data is collected for purposes of delivering targeted advertising -- rather than a discussion (even a clear one) that is buried within the privacy policy statement.[10]

---

[6] *Id.*

[7] FTC Privacy Roundtable, Dec, 7, 2009, Introductory Remarks of Chairman Jon Leibowitz, *available at* http://www.ftc.gov/speeches/leibowitz/091207privacyremarks.pdf.

[8] FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising – Behavioral Advertising Tracking, Targeting, & Technology (Feb. 12, 2009) *available at* http://www.ftc.gov/opa/2009/02/behavad.shtm.

[9] *Id.*

[10] *Id.* At 35-36.

This paper's proposal would achieve transparency in a much broader range of situations and would also be clearer and easier to read because consumers would not need to click on a link in order to receive information about a company's privacy practices. In addition, this paper's approach would provide consumers with information regarding the collection and use of data when that information is actually collected -- as opposed (in the example above) where the consumer is being notified *after the fact* that information was collected and is currently being used.

This paper's proposal also avoids consumer confusion by employing a simple and easy to understand color/number system with standardized bullet points that clearly and effectively inform consumers about data practices. This approach is consistent with FTC Commissioner Julie Brill's remarks at the 2010 "Conference of the Western Attorneys General" regarding "privacy 3.0,"[11] which stressed the importance of: "notice when new data collection practices or uses may result; simple, universal symbols that signal issues to consumers; and notice of unexpected/surprising uses."

The FTC Staff Report repeatedly expresses an overriding concern that consumer notice and choice is often ineffective because it is too complicated, not transparent to consumers, and does not enable meaningful choice.[12] This paper's proposal would provide clear, actionable information that consumers could act upon to exercise their privacy choices.

C. Early FTC Reports

In important respects, standardized, easy-to-understand privacy notices have been at the core of FTC efforts on privacy for more than a decade. Transparency has been a central feature of the FTC's policy statements regarding privacy in the Internet age. In the 1990's, in tandem with the Clinton Administration's e-commerce initiatives, the FTC engaged in broad business education efforts to encourage the posting of online privacy policies. Both of the FTC's reports to Congress on the state of online privacy protection emphasized the importance of easy to understand privacy notices.

In its first report to Congress on Internet privacy in 1998, "*Privacy Online: A Report to Congress*," the FTC wrote that: "*To be effective, [notice] should be . . . unavoidable and understandable so that it gives consumers meaningful and effective notice of what will happen to the personal information they are asked to divulge*."[13] In its 2000 follow-up Report, "*Privacy Online: Fair Information Practices in the Electronic Marketplace, A Report to Congress*," the FTC wrote that: "*Improving the clarity and*

[11] Commissioner Julie Brill, Federal Trade Commission, Remarks at Conference of the Western Attorneys General (July 18-21, 2010) (comments made in her own capacity and not necessarily reflecting the views of the FTC).

[12] Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, at iii-iv; 19-20; 25-28, 40, 52-53, 57-63, and 69-79 (Dec. 1, 2010).

[13] Privacy Online: A Report to Congress at 8 (June 1998).

comprehensibility of such policies . . . is essential to overcoming consumer concerns about the misuse of their personal information . . . [o]f utmost importance, privacy policies and other information practice disclosures should be clear and conspicuous, and written in language that is simple and easy to understand."[14]

D. White House Privacy White Paper

The White House Privacy White Paper, *Consumer Data Privacy In a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy,* released February 23, 2012, identifies as one of seven core privacy principles the principle that "[c]onsumers have a right to easily understandable and accessible information about privacy and security practices."[15] It explains that "companies should provide notice in a form that is easy to read on the devices that consumers actually use to access their services. In particular, mobile devices have small screens that make reading full privacy notices effectively impossible."[16]

E. FTC Privacy Report

The FTC's Privacy Report, *Protecting Consumer Privacy in an Era of Rapid Change,* released March 26, 2012, makes recommendations to companies and to Congress regarding protecting consumer privacy. It delves into greater detail regarding best practices to protect consumer information that would achieve the principles of the White House Privacy White Paper. The draft Report, issued for comment in December of 2010, observed that the current privacy framework has led to long, complex, and incomprehensible privacy policies that consumers cannot understand.[17]

The Final FTC Privacy Report's transparency principle is that "[p]rivacy notices should be clearer, shorter, and more standardized to enable better comprehension and comparison of privacy practices."[18] It concludes that "privacy statements should contain some standardized elements, such as format and terminology to allow consumers to compare the privacy practices of different companies and to encourage companies to compete on privacy." The FTC Privacy Report "calls on industry sectors to work together to develop standard formats and terminology for privacy statements applicable to their

[14] Privacy Online: Fair Information Practices in the Electronic Marketplace, A Report to Congress, at 27 (May 2000).

[15] Consumer Privacy in a Networked World, A Framework for Protection Privacy and Promoting Innovation in the Digital Economy, at 14 (Feb. 23, 2012).

[16] *Id.* at 15.

[17] Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, at iii, 19-20, 26-28, 44, 60, 70-72 (Dec. 1, 2010).

[18] *Id.* at 64.

particular industries," and observes that the Department of Commerce multi-stakeholder process "could be a useful venue to begin this exercise." The FTC Privacy Report notes specifically that "[m]achine-readable policies, icons, and other alternative forms of providing notice also show promise as tools to give consumers the ability to compare privacy practices among different companies."[19]

Moreover, the FTC Final Report also emphasizes the "urgency" of addressing this problem in the mobile environment, due to "the multitude of entities" collecting and using consumer information and the small space available for disclosures. It calls on "companies providing mobile services to come together and develop standard notices, icons and other means" so that the wide array of entities collecting information in the mobile environment can "communicate with consumers in a consistent and clear way."[20]

III. The Proposal: A Privacy Rating System and the Standardization of Privacy Notices

This paper advocates a two-phased approach that would promote transparency, would be easy for consumers to understand, and by doing so would enable consumers to make informed decisions about their personal information in a way that fulfills the FTC's recommendations. First, is a simple, standardized, transparent rating system for consumer privacy notices that can be implemented quickly, followed in a second phase by standardized privacy notice elements developed with industry input. This approach would address expeditiously and effectively the transparency and consumer empowerment interests that are at the core of both the FTC Privacy Report and the White House Privacy White Paper,[21] without chilling innovation or beneficial uses of consumer information. This approach would also complement "Do Not Track" mechanisms, while having much broader application.

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

A central concern of the draft[22] and final FTC Privacy Report,[23] as well as the White House Privacy White Paper,[24] is the degree to which consumer data is transferred and compiled into vast individual profiles in ways that most consumers do not understand and cannot control. For this reason, consumer privacy notices should clearly -- and in a standardized manner -- indicate the extent to which consumer

[19] *Id.* at 62.

[20] *Id.* at 63-64.

[21] *Id.* at 14-15

[22] *Id.* at i-ii, iv, 7, 9, 11, 13, 14, 20, 21-22, 23-24, 26-27, 30-33, 35, 37, 39, 46, 49-51, 54-55, 58, 61, 63, 69.

[23] *Id.* at 60-64.

[24] Consumer Privacy in a Networked World, at 12.

information may be disclosed for profiling when a consumer provides data to a business, non-profit, or governmental entity.

This paper proposes 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 greatest effectiveness, the privacy seal or icon should be prominently presented on the home page of the website and near the request for information. The icon designation would correspond to the key features of the privacy framework as follows:

1. A clear and conspicuous green seal or icon prominently featuring the number "1" would indicate that a commercial, non-profit, or governmental entity does not disclose consumer data or does so only for what the FTC's Staff Report calls "commonly accepted" practices;

2. A clear and conspicuous yellow seal or icon prominently featuring the number "2" would indicate that a commercial, non-profit, or governmental entity discloses information in ways that require consumer choice but that do not lead to proliferation of consumer data, or that disclose information in a format that cannot reasonably be re-identified; and

3. A clear and conspicuous red seal or icon prominently featuring 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 entity, such as a data broker, that in turn offers it for sale, exchange, or public disclosure, and would contain a very brief 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 already transparent to consumers. Thus, the practices described in the first and second categories should not, at this time, need an opt-out option. That said, we suggest that this system be adopted before such opt-out/opt-in options are decided. One of the significant benefits of this system is that it is very flexible and can be adapted quickly to evolving self-regulatory standards or rules and can incorporate additional options at a later time.

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 notice system would have 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 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 and avoiding imposition of a technology mandate; and

(f) fitting well with existing seal programs, while covering both behavioral advertising and other data sharing models. It bears considerable similarities to the Motion Picture Association of America's (MPAA's) movie rating system, whose success in educating the public points to the likely success of this model.

B. Phase Two: Standardized Privacy Bullet Points

The second phase would be to develop standardized, easy to understand points that would appear when the user clicked on the icon or seal, or on the next page of a written notice. This involves developing standardized bullets describing consumer data practices -- in place of longer standardized privacy notices because the standardization of privacy notices is far too complex and difficult to achieve in a short period of time. A directory of data collections, uses, and disclosures corresponding to these standardized bullet points would be created. This approach is much easier than standardizing privacy notices, and the bullets can be modeled after the FTC's proposed standardized descriptions.

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 standardize – that would eliminate legalese and use plain English so as to effectively and efficiently to provide consumers with information regarding data collection, use, and disclosure.

This rating-seal system would achieve, in a very flexible and scalable way, the core function of consumer transparency in providing consumer control. This rating-seal system would provide a foundation that both industry and policymakers could build upon as self-regulatory systems evolved because it could accommodate a range of features. For example, the rating-seal system could evolve to include additional features, such as additional opt-out and opt-in options – i.e., by adding categories relating to different opt-out or opt-in options, or some version of a "do not track" mechanism. However, the basic system as proposed would address consumer transparency and establish the foundation for basic

consumer control through informed decision-making, while at the same time facilitating greater consumer control later as consumer choice 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 a multi-stakeholder process of the sort described in the White House Privacy White Paper. That designation would then be considered a material statement to consumers that would be actionable under Section 5 of the Federal Trade Commission Act by the FTC 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 FTC for investigations and/or enforcement, just as the Better Business Bureau's National Advertising Division has long referred deceptive advertising cases to the FTC for further investigation and possible enforcement action.