Comments to the Department of Commerce Report
Commercial Privacy and Innovation in the Internet Economy:
A Dynamic Policy Framework (Green Paper)

Helen Nissenbaum, Professor, Media, Culture, and Communication & Computer Science
Kenneth Farrall, Adjunct Professor and Post-doctoral Researcher
Finn Brunton, Adjunct Professor and Post-doctoral Researcher
New York University
January 28, 2011

Observations:

Voluntary, enforceable codes of conduct can play a role in the emerging regulatory environment but are not sufficient. We agree with other respondents who have demonstrated that under the current regime, notice does not inform while choice is simply not choice.[1]

In our view, the Department of Commerce vastly overestimates the power of "enhanced transparency" in maintaining a healthy environment for personal privacy in the commercial context.

Consider, for example, the technological, institutional, and economic arrangements behind online behavioral advertising (OBA), which drives so much of the tracking activity that people find unacceptable. This is so *complex that it defies meaningful notice to general users* on matters that are crucial to privacy, for example, who the third party recipients are and what they do with the information they gather. Web content companies outsourcing advertising space are, themselves, often unaware of the types of information captured from their readers and customers or with whom the information is shared.[2] A user who decides to read a present day privacy policy would find that tracing the flow of his personal information can be an be an unending quest.

Transparency is further compromised by claims that certain data sets have been "anonymized," when the crucial terms are not subject to any standard definitions. Much has been written about the difficulty of *anonymization*. Our own research into one special case, that of Google's search engine cookie policy, illustrates the clear tradeoff between comprehensibility and specificity. The trouble with a comprehensible policy is that it can leave room for ambiguity. In the case we

[1] See "The Failure of Fair Information Practice Principles," by Fred H. Cate, ch. 13, *Consumer Protection in the Age of the Information Economy* (2006), and Aleecia M. McDonald and Lorrie Faith Cranor , "The Cost of Reading Privacy Policies, by, *I/S: A Journal of Law and Policy for the Information Society*, 2008 Privacy Year in Review.

[2] A recent UC Berkeley report, available online at http://www.knowprivacy.org, found that numerous companies that state they do not share information with third parties nevertheless have web bugs on their web pages used by third party ad firms. This is understood not to be an indictment of dishonesty of these companies but an indication of their lack of knowledge of the complexities of OBA practice.

studied, the policy was ambiguous enough to cast doubt on whether Google successfully "anonymizes" search logs.[3]

The term "opt out," too, is highly ambiguous, unclear as to whether the user has opted out of profiling, tracking or both. Since Microsoft and Yahoo networks, for example, use unique ID cookies to register opt outs, users are exempting themselves from targeting but not tracking. In other cases, decisions to opt-out may not be honored across ad networks or when back-up systems like flash cookies provide the same function.

Finally, there is an egregious loophole in *notice of change* in privacy policies. Current practice places discretion in the hands of website owners, while the onus is on users to stay abreast.

In sum: The role consumers are expected to play in the current notice and choice regime is unsustainable and illogical.[4]

Recommendations:

We support the DoC direction of FIPPS enhanced with specific substantive requirements. Among others, we recommend the following:

Key terms: Mandated, peer-approved definitions and standards for terms, such as anonymization, which are critical to a common and accurate understanding and evaluation of privacy practices.

Policy Changes: Substantive restrictions on how policies may be changed, including peer-approved, mandated standards for notifying users; our preference is for prominently displayed, "opt-in" mechanisms. Upon learning of changes in a particular entity's privacy practices, users should ALWAYS be given the option of deleting all personal information from the entity's databases.

Sector-related (contextual) requirements: To relieve the impossible burden on general users of Transparency-and-Choice regimes, as well as inequalities of bargaining positions inherent to it, we recommend the formulation of baseline substantive constraints on data practices following the model of current US sectoral privacy regulation. These sectoral rules should be extended into online interactions to cover aspects of online interactions that fall outside the scope of existing rules (e.g. under GLBA privacy rules, or the Video Privacy Protection Act, FERPA, etc.). Instances of this might be, IP address, clickstream, web-surfing histories, which may not be have been covered or even considered by such statutes (and associated rules).

---

[3] V. Touibana and H. Nissenbaum (forthcoming in The Journal of Privacy and Confidentiality), "Analysis of Google Logs Retention Policy."

[4] For an extended discussion see S. Barocas & H. Nissenbaum, "On Notice: The Trouble with Notice and Consent," Proceedings of Engaging Data Forum: The First International Forum on the Application and Management of Personal Electronic Information, Oct. 2009. http://www.nyu.edu/projects/nissenbaum/papers/ED_SII_On_Notice.pdf

We recommend heuristics, such as those developed in Helen Nissenbaum's book, *Privacy in Contex*t,[5] that look to context-specific informational norms to guide adoption of appropriate privacy rules. Within certain contexts, (e.g. in the commercial marketplace, healthcare, education, etc.) some of these norms might deserve to be embodied in enforceable rules while others might be recommended standards of good practice. These norms specify the types of information being collected, the role of information subject, with whom this information is being shared, and subject to what conditions (i.e. principles of transmission.). It is easy to see that behavioral advertising violates long-standing norms of information flow in many of the contexts in which it is used.

A challenge of this approach is to provide guidance on the contexts to which particular websites belong. This is not likely to be easy but neither is the equivalent task that has been undertaken in the United States for pre-existing business enterprises and institutions. The fact that a web-based enterprise supports itself through private payments or advertising ought not exempt it from internal standards of its sphere of operation.

Enforcement: Enforcement of explicit sector (context) specific baseline requirements, change policies, and standardized definitions of key terms must be anchored in legislation, at the very least, legislation that grants necessary enforcement power to the FTC, or some other appropriate government body. The FTC currently has limited regulatory authority without Congress extending this via legislation.

User-driven privacy enforcement: We support further exploration of "Do not track" mechanisms. We also urge support for design alternatives that serve privacy interests with consideration for commercial growth. One example is *Adnostic*, an ad delivery technology developed jointly at New York University and Stanford University, which enables targeted advertising within a user's browser.[6] Adnostic may appeal to consumers who would block advertising altogether and provide advertising revenue to websites avoiding targeted advertising to protect visitors against third-party tracking.[7] Such forms of privacy innovations should be encouraged and protected.

---

[5] Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford: Stanford University Press.

[6] Work on Adnostic has been supported by the NSF PORTIA and by the MURI program under AFOSR Grant No: FA9550-08-1-0352.

[7] For an extended discussion of Adnostic, see V. Toubiana, A. Narayanan, D. Boneh, H. Nissenbaum, and S. Barocas, "Adnostic: Privacy Preserving Targeted Advertising," Proceedings Network and Distributed System Symposium, March 2010. http://crypto.stanford.edu/adnostic/adnostic.pdf