

1001 G Street, N.W.
Suite 500 West
Washington, D.C. 20001
tel. 202.434.4100
fax 202.434.4646

Writer's Direct Access
Sheila A. Millar
(202) 434-4143
millar@khlaw.com

January 28, 2011

Via Electronic Mail: privacynoi2010@ntia.doc.gov

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW
Room 4725
Washington, DC 20230

Re: Docket No. 101214614-0614-01

Dear Sir:

On December 16, 2010, the Internet Policy Task Force (“IPTF”) of the Department of Commerce (DOC) released a “Green Paper” report on privacy, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*, and an associated Federal Register notice, *Information Privacy and Innovation in the Internet Economy*, 75 Fed. Reg. 80042 (Dec. 21, 2010), soliciting comments on the Green Paper. Having worked with many clients on privacy-related issues, we offer the following reactions to some of the concepts raised.

Baseline Fair Information Practice Principles (FIPPs) already exist and are widely practiced by businesses, but the Green Paper’s discussion of “enhanced” FIPPs assumes a level of consensus on aspects of privacy that does not exist in practice. Major businesses have recognized and adopted FIPPs into their day to day operations, recognizing that collection and use of different types of information creates different issues. “Data” is not monolithic, one reason that the U.S. privacy legislation has focused on sectoral privacy laws. Harms or risks associated with collection and use vary, so one-size-fits-all privacy standards will not work. Indeed, some of the framework concepts may in fact be inconsistent with current law, as noted below.

The Green Report’s discussion of a framework commercial privacy law is therefore premature, and is in striking contrast with the President’s recent call for action to reduce regulatory burdens on industry. Distinctions between personal and non-personal data are essential to the functioning of business operations in some contexts, for example, while in others, as with online behavioral advertising (OBA), those distinctions may be less important. For that reason a robust program of self-regulation has been developed and a voluntary enforcement component has been recently launched with the support of major advertising industry organizations to address OBA.

Thus, it is not apparent that a “multistakeholder” process to develop codes of privacy practice is necessary or appropriate. Self-regulation is effective because businesses share concerns about protecting privacy and can work expeditiously to implement programs that reflect practical operational details that framework policies are not capable of addressing. That is not to say that self-regulatory programs develop in a vacuum, but that input from non-business stakeholders may be obtained in many different ways. For DOC to suggest that a particular form of “self regulation” should be mandated suggests an entirely different and more cumbersome approach akin to a negotiated rulemaking. Any proceeding that involves government mandates must occur through traditional rulemaking processes and procedures that accord all participants the appropriate procedural and statutory protections.

Existing privacy self-regulatory initiatives respect and recognize existing laws on privacy. However, a “Do Not Track” feature may in fact be inconsistent with current law. The Children’s Online Privacy Protection Act (COPPA), for example, does not permit websites or online services to create or maintain a database of information about children absent verifiable parental consent. To create such a database would require collecting more information from parents and children. This is an example of possible inconsistencies resulting from the flawed concept of a national Do Not Track system.

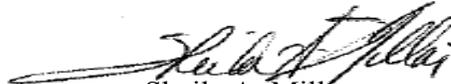
The Green Report does not necessarily make the case for the need to create a Privacy Policy Office. To the extent such an office would be useful and can be funded in keeping with the desire to reduce regulatory burdens and shrink government, the focus should be on assisting U.S. businesses in addressing barriers to trade from foreign privacy laws that purport to restrict the transfer of data to the U.S.

Finally, the suggestion that more should be done to promote use of Privacy Impact Assessments (PIAs) and to make them transparent reflects another concept that appears flawed. PIAs may be a useful internal tools but should not be mandated or required to be publicly disclosed. They are not universally used nor are they likely to be needed in all cases. Where they are used, PIAs may contain confidential business information or disclose information that could disclose data security limits, potentially increasing the vulnerability of data to exposure.

U.S. Department of Commerce
January 28, 2011
Page 3

Thank you for the opportunity to submit these views.

Sincerely,



Sheila A. Millar

cc: Aaron Burstein, Office of Policy Analysis and Development,
National Telecommunications and Information Administration
U.S. Department of Commerce
aburstein@ntia.doc.gov

Manu Bhardwaj, Office of Policy Analysis and Development,
National Telecommunications and Information Administration
U.S. Department of Commerce
mbhardwaj@ntia.doc.gov