February 2, 2010

TO: The Honorable Gary Locke, Secretary of Commerce
The staff and members of the Internet Privacy Task Force

FROM: Comradity, www.comradity.com
Katherine Warman Kern, katherine@comradity.com; 203-918-2617

Who would argue with the intent of the Internet Privacy Task Force, broadcasted in the December 16, 2010 press release of a green paper: "Commerce Department Unveils Policy Framework for Protecting Consumer Privacy Online While Supporting Innovation?" But we all know how difficult it is to execute potentially conflicting objectives. And the green paper fails to overcome this challenge.

The "Dynamic Policy Framework" is comprehensive and thoughtful, but fails to offer "a clear lens through which to assess current policy" (Foreward by Cameron Kerry, pp. iv) because the leadership level communication is contradictory and confusing relative to the detail discussion. While I understand the need for "dynamic" somewhere in policy making, the framework should be consistent and clear, so the execution can be dynamic and still have fundamental integrity.

For example, there are contradictions in the goals set in Secretary Locke's introductory letter and the Foreword from General Counsel Kerry.

The paper begins with a letter from Secretary of Commerce, Gary Locke, in which he clearly states there is a problem from the consumer point of view, compelling a "fresh look:"

New devices and applications allow the collection and use of personal information in ways that, at times, can *be contrary to many consumers' privacy expectations*. Addressing these issues in a way that protects the tremendous economic and social value of the Internet without stifling innovation *requires a fresh look at Internet policy (emphasis mine)*.

However, Cameron Kerry, General Counsel, asserts that the current model builds trust and protects consumers:

The United States has developed a model that facilitates transparency, promotes cooperation, and strengthens multistakeholder governance that has allowed innovation to flourish while building trust and protecting a broad array of other rights and interests.

As a result of the task force's satisfactory assessment of the status quo, Kerry asserts that the goal of the task force is to ***maintain*** consumer trust:

Privacy protections are crucial to maintaining the consumer trust that nurtures the Internet's growth.

And instead of taking a fresh look, the recommendation is to "reinvigorate" transparency:

. . . the green paper recommends reinvigorating the commitment to providing consumers with effective transparency into data practices, and outlines a process for translating transparency into consumer choices through a voluntary, multistakeholder process.

In other words, Kerry presumes that consumer trust is "good enough" when third parties are transparent about taking raw data without consumers' express consent, interpreting it without consumers' corroboration and participation , yet representing that interpretation as actionable and expected by consumers to Vendors, for commercial purposes.

The assertion that consumer trust is satisfactory contradicts both Secretary Locke and the body of the greenpaper, which cites research revealing consumers of all ages do not trust these commercial uses of their information. Separately, despite the representation of consumer marketing companies in the list of inquiry respondents, there is little reference anywhere to the industry's desired improvement in the effectiveness of internet marketing tools and media. How can the Commerce Department ignore that the fastest growing segment of the Internet is "custom digital publishing"? Marketing companies like Procter and Gamble are taking a detour around media companies to connect with consumers and are producing their own media properties to build relationships. This is specifically because marketing professionals realize that growing the business through short term promotions is not as effective nor as efficient as building long term relationships with consumers.

Instead of advocating for the status quo and endorsing current practices through regulation and policy – as if this is the best business can do to both build consumer trust and promote innovation - the government should "disrupt ambiguity" with policies which encourage innovation that IMPROVES consumer trust, relationship building with commercial enterprises, and consequently the value of information to develop, market, and communicate with consumers.

There are many initiatives working to achieve these objectives. For example, Project VRM, and the Personal Data Ecosystem. It is hard enough for entrepreneurs in these communities to raise investment dollars and educate consumers in today's highly competitive market. We wonder why the government would endorse or sanction existing practices as "best" making it even more difficult for these initiatives to overcome hurdles for success.

In the spirit of promoting innovation to improve consumer trust, here's Comradity's opinion on the greenpaper's recommendations and response to the questions posed in the green paper.

As background, the paper's "Dynamic Privacy Framework" makes 4 recommendations:

1. **Fair Information Practice Principles (FIPPs):** "clearly articulated **purposes** for data collection, commitments to **limit data uses** to fulfill these purposes, and expanded use of robust **audit systems to bolster accountability**."
2. **Privacy Policy Office in the Department of Commerce (PPO):** "work with the FTC in leading efforts to develop voluntary but enforceable codes of conduct. Companies would voluntarily adopt the appropriate code developed through this process. This commitment, however, would be enforceable by the Federal Trade Commission. Compliance with such a code would serve as a safe harbor for companies facing certain complaints about their privacy practices."
3. **Encourage Global Interoperability:** "build on accountability, mutual recognition and reciprocity, and enforcement cooperation principles pioneered in the Organisation for Economic Cooperation and Development (OECD) and Asia-Pacific Economic Cooperation (APEC)."
4. **Ensure Nationally Consistent Security Breach Rules:** "Federal commercial data security breach notification (SBN) law that sets national standards, addresses how to reconcile inconsistent State laws, and authorizes enforcement by State authorities. . .The FTC and individual States should have authority to enforce this law."

Here is Comradity's response to each of these recommendations:

1. The value of the FIPPs is directly related to whether the goal is to maintain consumer trust or improve it. For example, we believe that if the default were "opt-in" instead of "opt-out", companies would be naturally inclined to be transparent and limit data uses to those that clearly and directly benefits the consumer in order to increase "opt in" rates. To avoid potentially deceptive or empty promises, we believe an independent multi-stakeholder agency review (e.g., the Privacy Impact Assessment (PIA) ratings) would assure audit systems are used to prevent drops in PIA ratings. To encourage new companies or existing companies who are innovative to make such a dramatic shift, why not give companies a free pass on regulations or favorable tax incentives when they make the default "opt-in" and volunteer for the PIA ratings? (For more of our thoughts about FIPPs, see our responses below to the detailed questions posed about FIPPs by the Task Force in Appendix A).
2. Why recommend adding the PPO, another representative to represent business interests? If there's a need for a new government agency, shouldn't it be a multi-stakeholder representative agency with representatives from Commerce, the FTC, the new Consumer protection agency, individual States Attorney Generals, the State Department, and others?
3. If the objective of the Department of Commerce is to encourage global interoperability, why does it fail to acknowledge the existence of Privacy Commissions in Europe and Canada? In fact, another example of the contradictions between different sections of the greenpaper, in the body of the discussion about FIPPs, Privacy Impact Assessments (PIAs) are recommended, following the example of the European Commission:

   > An industry standards organization pointed to the example of PIAs for radio frequency identification (RFID) tags, readers, and writers; 106 the European Commission recommended that EU Member States and RFID users develop a framework to assess the privacy risks (and safeguards) of using RFID applications.

4. It's expected that the Department of Commerce will advocate nationally consistent rules across all states, but instead of mandating state compliance, why not engage the states to participate in the collaborative process the Department of Commerce purports to be executing through the Internet Privacy Task Force?

Here are Comradity's specific responses to the Department of Commerce Internet Privacy Task Force Green Paper questions regarding the FIPPs:

(From Appendix A: pp. 70-71)

2. To meet the unique challenges of information intensive environments, FIPPs regarding enhancing transparency; encouraging greater detail in purpose specifications and use limitations; and fostering the development of verifiable evaluation and accountability should receive high priority.

a. What is the best way of promoting transparency so as to promote informed choices? The Task Force is especially interested in comments that address the benefits and drawbacks of legislative, regulatory, and voluntary private sector approaches to promoting transparency.

RESPONSE: *The hurdle to transparency is the ultimate exit strategy for most internet start-up companies. In order to maximize value, investors want open-ended terms to use personal data*

in the context of both time and re-sale to multiple levels of parties. That's why most privacy policies assert the broadest possible terms and the default is opt-out (consumers must opt-out if they do not want to participate). In my opinion, legislating an opt-in default (consumers must opt-in for their data to be used), requires companies to be identify terms of use and purposes which are compelling and relevant to the consumer.

b. What incentives could be provided to encourage the development and adoption of practical mechanisms to protect consumer privacy, such as PIAs, to bring about clearer descriptions of an organization's data collection, use, and disclosure practices?

RESPONSE: *In lieu of a Privacy Policy Office in the Department of Commerce, representing business interests, wouldn't a new independent multi-stakeholder representative agency that publishes PIAs be more valuable to everyone?*

c. What are the elements of a meaningful PIA in the commercial context? Who should define these elements?

RESPONSE: *In a market where the goal is to improve consumer trust, the bar should be constantly improving and therefore the rating system needs to be dynamic enough to reflect changing standards both in the US and Internationally.*

d. What processes and information would be useful to assess whether PIAs are effective in helping companies to identify, evaluate, and address commercial data privacy issues?

RESPONSE: *A new independent multi-stakeholder representative agency should have representatives from the Dept. of Commerce, the new Consumer protection agency, the FTC, and the State Department's liaison with International Privacy Commissions. An annual state of consumer trust report should be published, generating ratings for overall consumer confidence as well as specific companies and institutions. The criteria for the ratings should be dynamic reflecting continuous improvement in standards.*

e. Should there be a requirement to publish PIAs in a standardized and/or machine-readable format?

RESPONSE: *This should be the responsibility of the new agency and be consistent across other International Privacy Commissions.*

f. What are consumers' and companies' experiences with systems that display information about companies' privacy practices in contexts other than privacy policies?

RESPONSE: *This is almost laughable as an objective given the current constant revisions to privacy policies and terms of use and lack of standards.*

g. What are the relative advantages and disadvantages of different transparency-enhancing techniques in an online world that typically involves multiple sources being presented through a single user interface?

RESPONSE: *When we know what the different transparency-enhancing techniques are we can assess these.*

h. Do these (dis)advantages change when one considers the increasing use of devices with more limited user interface options?

RESPONSE: *See above response.*

i. Are purpose specifications a necessary or important method for protecting commercial privacy?

RESPONSE: *Purpose or intent is essential to protecting everyone's assets – commercial or personal.*

j. Currently, how common are purpose specification clauses in commercial privacy policies?

RESPONSE: *See next response.*

k. Do industry best practices concerning purpose specification and use limitations exist? If not, how could their development be encouraged?

RESPONSE: *There are no best practices. Since the default is opt-out no one is compelled to devise purposes and limitations which both benefit the consumer and generate profit, they only consider commercial benefit to themselves or others. As discussed above the best way to encourage transparency to improve consumer trust is to legislate/regulate opt-in as the default for using consumer information.*

l. What incentives could be provided to encourage companies to state clear, specific purposes for using personal information?

RESPONSE: *When they make more money by doing it.*

m. How should purpose specifications be implemented and enforced?

RESPONSE: *By making opt-in the default and using PIA's to publicize participation rates and performance ratings.*

n. How can purpose specifications and use limitations be changed to meet changing circumstances?

RESPONSE: *By asking customers if they would opt-in to a change.*

o. Who should be responsible for demonstrating that a private sector organization's data use is consistent with its obligations? What steps should be taken if inconsistencies are found?

RESPONSE: *The multi-stakeholder agency which reports the PIAs should be responsible. Companies should be required to make their PIA rating accessible on every page of their website along with their privacy policy and terms of use.*

p. Are technologies available to allow consumers to verify that their personal information is used in ways that are consistent with their expectations?

RESPONSE: *There has been no reason to create this application, but technologies exist to build from.*

q. Are technologies available to help companies monitor their data use, to support internal accountability mechanisms?

RESPONSE: *Same as above.*

r. How should performance against stated policies and practices be assessed?

RESPONSE: *The proposed PIAs should do this to build its ratings. And consumer research should be done to verify.*

s. What incentives could be provided to encourage companies to adopt technologies that would facilitate audits of information use against the company's stated purposes and use limitations?

RESPONSE: *If the default is opt-in rather than opt-out and an independent agency were generating PIA ratings on a regular basis that are accessible on every page of a website and could impact opt-in rates, companies would be very incented to monitor performance to avoid a surprise.*