January 28, 2011

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Ave., N.W., Room 4725
Washington, D.C. 20230

RE: Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework, RIN 0660-XA22

Dear Internet Policy Task Force:

General Electric (GE) appreciates the opportunity to submit comments on the U.S. Department of Commerce's report entitled "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework" (the "Green Paper").

GE operates in more than 100 countries, with over 300,000 employees worldwide. As custodians of the personal data of our workforce as well as trusted guardians of consumer data, GE is committed to robust privacy protection of the personal information we maintain. We agree with the Green Paper's recognition that a stronger privacy framework is key to promoting consumer trust and support the Task Force's efforts to establish an effective and efficient system of privacy rules. In particular, we strongly support the Green Paper's recommendations for consistent privacy standards internationally. As a multinational company that has been a leader in privacy and data protection around the globe, we believe that the lack of consistent standards globally is a major obstacle faced by multinational organizations in maintaining enterprise-wide privacy standards. We have provided comments on specific Green Paper recommendations below.

I. Creating a Stronger Privacy Framework

GE supports the development of uniform privacy rules, which would serve the two main goals of the Task Force's – promoting consumer trust in the Internet economy and promoting innovation. We agree that a stronger privacy framework would promote increased protection for consumers while providing certainty to businesses. GE supports the Task Force's focus on increasing commercial

compliance with revitalized Fair Information Practice Principles (FIPPs) as a means to achieving a more uniform framework for data protection. As a leader in data protection, GE has incorporated FIPPs into its daily business practices. We specifically support the Task Force's recommendations for the development of FIPPs focused on the following[1]:

(1) Enhancing transparency. We agree that lengthy and complex privacy notices may not adequately inform consumers of a company's uses and disclosures of their personal information. We support efforts to provide guidance on how to make these notices more accessible, clear and meaningful to consumers. Properly implemented, this will increase consumer trust. Based on our experience through our financial services business, regulated by the Gramm-Leach-Bliley Act, GE believes that government-sanctioned uniform privacy notices would serve to protect consumer rights while at the same time creating certainty for businesses. GE also agrees that, as a complementary approach, performing Privacy Impact Assessments (PIAs) should be an integral part of every company's data privacy practices, and companies should integrate PIAs and other Privacy Design principles into their data practices.

(2) Purpose specification and use limitations. As a complement to greater transparency, GE agrees with the Task Force's recommendations that purpose specification principles and use limitations provide greater clarity and privacy protection for consumers. We view these principles as a logical extension of transparency, requiring companies to provide clear statements of their practices and to adhere to these statements in using personal information. Obviously, purpose specification and use limitations must remain flexible, to account for the realities of how a particular company must operate and as understood by consumers.

(3) Auditing and accountability. We agree with the Task Force's observation that auditing and accountability play a critical role in ensuring that transparency, purpose specification and use limitation practices are carried out. GE supports FIPPs that include a strong audit and accountability component. This helps to ensure that a company's data use is consistent with its stated obligations. We believe that a routine part of ensuring adequate data protection is to assess one's performance against stated policies and practices. We believe that businesses should not only comply with the law, but that compliance should be visible and prominent as a priority.

Together these three principles as part of a FIPP framework will help to ensure that companies collect, process and use personal data for legitimate business purposes and provide clear notice to consumers about their practices. These principles also are consistent with the European Union principles; this may help to better foster international standards, which we also believe is an important goal in re-thinking United States data protection standards.

---

[1] Green Paper Recommendation #2.

II. Voluntary and Enforceable Codes of Conduct

GE supports an approach that allows for self-regulatory efforts combined with clear enforcement mechanisms, as recommended by the Green Paper.[2] In particular, we believe that any legislation should allow for a safe harbor for commercial entities that have adopted widely accepted industry best practices. A safe harbor that is enforceable by regulatory agencies will provide industry with the ability to address emerging technologies. Providing a safe harbor for companies that adhere to a voluntary code of conduct also will help to provide incentives to develop such codes of conduct. We also support the creation of a Privacy Policy Office within the Department of Commerce to assist in the development of effective, consensus-based voluntary codes of conduct in different commercial contexts.

III. Global Interoperability

GE strongly supports the Task Force's recommendation that the U.S. government should continue to work toward increased cooperation among privacy enforcement authorities globally. We believe it is imperative that the U.S. work toward developing a framework for mutual recognition of commercial data privacy framework in other countries.[3] GE appreciates the need for a singular, coordinated approach by multinational companies. A concerted effort to facilitate cooperation with other countries' commercial data privacy frameworks can help ease the burden on multinational companies so they can focus less of their resources on multi-jurisdictional privacy compliance and more on innovation.

One of the most challenging aspects of data protection and management is the disparate approaches to commercial data privacy across national borders. As a multinational company that manages employees and consumer data across 100 different countries, GE experiences first hand the significant costs to businesses of non-harmonized data protection rules. We believe that an enhanced U.S. privacy framework will better facilitate greater harmonization of standards and international interoperability.

As an early adopter of Binding Corporate Rules (BCRs), GE remains at the forefront of privacy and data protection. BCRs, as a set of rules adopted within a company that provide legally binding protection for data processing within the company, can provide a meaningful mechanism for promoting global interoperability. We believe that BCRs represent one of the most promising ways of assuring safe cross-border flows within multinational groups. The BCR process remains extremely burdensome and complex despite attempts at streamlining the process, and we believe that simplifying the process, such

---

[2] Green Paper Recommendation #3.

[3] Green Paper Recommendation #6.

as through further expansion of mutual recognition agreements, or other consolidated programs will be important to facilitating international standards for data protection.

IV. Nationally Consistent Security Breach Notification Rules

We also appreciate the Task Force's recognition of the challenges of complying with multiple rules within the U.S.[4] In particular, GE supports a national data breach notification rule that preempts state laws. A comprehensive national approach to data breach notification would provide consistency for consumers as well as for businesses. We believe that a federal law that provides for preemption of state laws governing the same subject matter would help to ease the compliance burdens for companies attempting to track and comply with an ever-changing state law landscape regarding breach notification. A uniform federal law can provide certainty to businesses and consumers.

In many cases, duplicative state laws add compliance burdens without adding protections to consumers. Under the current system, multistate companies are subject to different and sometimes contradictory rules regarding when notification is required in the case of a data breach. Further, because data breaches rarely concern data subjects located only in one state, complex questions arise about which law applies. For example, if a data breach occurs in California, yet some of the subjects live in Massachusetts, which state law applies?

GE also supports the inclusion of a risk of harm standard in any federal security breach notification framework. In the context of data breaches, a distinction should be drawn between the duty to notify regulators and the duty to notify data subjects. It is important to notify data subjects when there is a significant risk that their data may be misused; notification absent such potential harm offers consumers little value and may undermine the very goal of notification.

V. ECPA Reform

GE supports the Task Force's recommendation that the Electronic Communications Privacy Act (ECPA) be updated to better reflect changes in technology that have occurred since the law's enactment.[5] We agree that the ECPA should be reviewed to address privacy protections in a number of newer contexts, including cloud computing and location-based services. The ECPA will better protect privacy if it reflects current technology. GE supports revisions to ECPA to give consumers more protection from contemporary privacy violations while clarifying rules for businesses developing new technology not contemplated when the law was drafted, such as GE's smart grid technology.

---

[4] Green Paper Recommendation #7.

[5] Green Paper Recommendation #10.

Conclusion

GE appreciates the opportunity to submit comments on the Green Paper. We support the work of the Task Force, and we believe that the Dynamic Policy Framework proposed by the Green Paper is an important step in creating a national uniform privacy framework that encourages innovation while protecting consumers.

Sincerely.

Nuala O'Connor Kelly
Chief Privacy Leader and Senior Counsel, Information Governance
202 637 4151
nuala.oconnorkelly@ge.com