



**Department of Commerce Internet Policy Task Force Report**  
***Commercial Data Privacy and Innovation in the Internet Economy:***  
***A Dynamic Policy Framework***  
**Docket No. 101214614-0614-01**

**GS1 Comments**  
**28 January 2011**



**Re: GS1 US comments on the Department of Commerce Internet Policy Task Force Report on *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework* (Docket No. 101214614–0614–01)**

GS1 US is one of 108 country-based Member Organizations of GS1. GS1 is a global organization dedicated to the development of standards and solutions to improve the efficiency and visibility of supply chains and demand chains, both globally and across industries. More than one million companies use GS1 standards to do business across 150 countries. GS1 and its subsidiaries and partnerships connect companies with standards-based solutions that are open and consensus-based.

GS1 US member companies represent more than 200,000 American businesses in more than 20 industries including consumer packaged goods, grocery, apparel, government, aerospace, retail, foodservice, healthcare, fresh and packaged foods, consumer electronics and high-tech. Some of the world's largest corporations participate in our boards and work groups, motivated by the knowledge that GS1 standards help their companies reduce costs and increase both the visibility and security of their supply chains.

GS1 US participated in the earlier Department of Commerce request for comment on Privacy and Innovation in the Internet Economy, and we appreciate the manner in which the Department has taken into account our suggestions.<sup>1</sup> We believe that the Green Paper will add to the unprecedented dialogue which is taking place on privacy, not only within the Department, but also through the European Commission's *Consultation on Personal Data Protection* and the Federal Trade Commission's proposed *Framework for Protecting Consumer Privacy*.

The very fact that these documents have been issued at this time reminds us of the need to develop privacy policies that will be globally interoperable, and we support the Department in its efforts to achieve that end. **As an organization devoted to the development of standards that allow for global interoperability, we fully understand the importance of applying the interoperability requirement in the public policy domain as well.**

We will focus these comments on what we have learned from our participation in the development of the Framework for a Privacy Impact Assessment (PIA) for RFID Applications, which was called for in the *European Commission Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification*.

**As the Department points out, PIAs can play a valuable role as part of a dynamic policy framework.** They require companies to think carefully about privacy as they create and implement new products and services. PIAs support the application of "privacy by design," allowing products and services to have privacy protections "baked in." This approach helps to reduce the costs incurred when products and services must be retrofitted due to privacy concerns raised after a new product or service is released. PIAs should facilitate extending privacy awareness throughout an organization rather than leaving it in a policy "silo," to increase the likelihood of the development of an organization-wide privacy promoting culture. PIAs also promote accountability for decisions about products and

---

<sup>1</sup> <http://www.ntia.doc.gov/comments/100402174-0175-01/attachments/GS1%20EPCglobal%20Comments.pdf>

services that may impact privacy, and they encourage the development of workable self-regulatory regimes.

We support the appropriate use of PIAs for these reasons and more, but our experience in the year-long process that led to the development of the European PIA Framework has provided us with some cautionary lessons as well.

**One reason for the success of the European process was that the European Commission served in a convening role that ensured broad industry participation. Such a convening role could also be played by the new Privacy Policy Office within the Department.**

After kicking off the process the Commission relied upon industry to formulate the Framework. Letting industry take the lead ensured that the Framework reflected real world conditions and actual business policies and practices. This increased the likelihood that the Framework could be efficiently and effectively implemented. Even so, it appears likely that some level of customization would still be beneficial for different industry segments. From our industry discussions we have learned that “one size does not fit all.”

The Commission encouraged broad consultation by industry, and the dialogue that extended beyond industry was very helpful in improving the quality of the Framework that was eventually proposed. We agree with the Department’s approval in the Green Paper of a multi-stakeholder approach, **but we believe it is important that those who must take responsibility for the implementation of the PIA should also take the lead role in designing it, while still reaching out to others.**

At the core of the PIA process is the effort to identify the threats, if any, to privacy posed by the new product or service, to determine the likelihood of the threats, and to evaluate the risks the threats pose to privacy. When the likelihood of the threat and the severity of its consequences are understood, it is much easier to determine what actions should be taken to mitigate the risks, if any. In many cases these are not simple tasks.

We think this kind of analysis is very important and very useful, not only to the company but to its customers and society at large. However, the analysis is not intended as a response to the principle of transparency. A PIA is not the company’s statement of its privacy policy. Instead, it is a means to increase the likelihood of fulfilling all the Fair Information Practices principles, as all the principles should be considered part of the analytic process.

**We do not believe each PIA should be required to be published.** A company’s policies on privacy should be clear, concise, and transparent. Yet requiring that each PIA be published could chill internal discussions and subject every analytic decision to a continuing series of debates as well as force the disclosure of confidential business information. A publication requirement would actually detract from the more appropriate focus on the company’s stated privacy policies and whether it lives up to them, as well as the end result of the PIA process, which is the product or service that is actually implemented. The proof, as the saying goes, is in the pudding, not the cooking instructions.

**Because a PIA can be expensive and time consuming, it is important to take considerable care to design the processes to be used so as to make the PIA cost effective.** This is particularly true regarding small and medium-size enterprises that possess constrained resources and which do not have staff dedicated to public-policy activities. For

the same reason, a PIA should not be required for every decision that might affect privacy; a multi-stakeholder process might provide a vehicle for giving input to the Department for when a PIA would be most appropriate and cost effective. This could then be the basis of a best-privacy practice. We suggest that PIAs are most appropriate when threats to privacy interests are both likely and serious.

While we do not believe PIAs should be required, nor that they should be made public, we do think that they might be useful in an additional way. If a company is challenged with respect to its activities, it should be able to use a PIA to demonstrate that it carefully considered the privacy implications of its actions and came to a reasonable decision. This would not excuse behaviors that violate applicable laws and regulations, but in other cases could demonstrate a reasonable degree of care was taken on the part of the company.

**We strongly support the Department's emphasis on the need for the global interoperability of privacy policies.** We have seen this issue arise with respect to the PIA Framework in Europe. As we have told the European Commission, we are concerned that, even with an agreed upon Framework, it is uncertain how the various member states of the European Union will treat the PIA process. That uncertainty and the potential for multiple and conflicting responses is particularly threatening for those companies providing products and services in multiple member states. This same comment applies to the need for policy interoperability among the nations of the world and among the various political subdivisions such as states in the United States.

**We strongly endorse the Green Paper's emphasis on privacy principles.** These principles have proven their lasting value over the last 30 years, even while the mechanisms to give them operational meaning have had to evolve to reflect changes in technology and in the uses of information. **We similarly endorse the need for flexibility in responding to changing circumstances which the Department has aptly captured.**

**One example of the need for flexibility can be seen in the emergence of what has become known as the Internet of Things.** This idea of millions, billions, and even trillions of devices communicating with one another is no longer something confined to science fiction. We raise the Internet of Things because of our work with RFID technology and because some observers have mistakenly equated the Internet of Things with the use of RFID technology. We predict that over time the preponderance of objects that communicate will do so with sensors, the kind of device that might be employed to control electricity use in buildings, monitor borders, inform us of the state of our bridges, collect climate information in sensitive environments, or even to monitor for radioactivity or bioterrorism. Because of the potential linkage between the data broadcast by autonomous and semi-autonomous sensors and personally identifiable data, there may well be privacy concerns.

One way of responding to this possibility is to impose a notice-and-consent regime, yet it is hard to imagine posting notices or providing choices in many of these situations. It may not be desirable, or even possible, to effectively implement access requirements. It is difficult to consider how data minimization or purpose specification would operate if the goal is to gather a wide range of data and analyze it in an effort to find new insights for the greater good.

If one goes back to the privacy principles it may be that the purposes of privacy protection can be achieved by looking at enforceable use limitations rather than simply assuming that the full range of mechanisms we have used in the past will be necessary and appropriate to every new development. We believe the Internet of Things requires new thinking and

flexibility so that we can benefit from its capabilities while protecting the privacy of personally identifiable information.

Once again we would like to express our appreciation for the thoughtful work of the Department of Commerce and for allowing us to participate in this dialogue. We look forward to continuing to work with other stakeholders in the important work of protecting privacy, fostering innovation and enhancing global commerce. We hope that the global perspective that we bring will help lead to the global policy interoperability that both we and the Department are seeking.

For more information, please contact:  
Elizabeth Board  
Executive Director, GS1 Global Public Policy  
1101 30th St., NW Suite 500  
Washington, DC 20007  
[elizabeth.board@gs1.org](mailto:elizabeth.board@gs1.org)  
[www.DiscoverRFID.org](http://www.DiscoverRFID.org)  
[www.GS1US.org](http://www.GS1US.org)  
[www.GS1.org](http://www.GS1.org)  
[www.EPCglobal.org](http://www.EPCglobal.org)  
[www.EPCglobalUS.org](http://www.EPCglobalUS.org)