Federal Trade Commission Preliminary Staff Report
Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers

GS1 US Comments
18 February 2011

Re: GS1 US Comments on the Federal Trade Commission Preliminary Staff Report *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers.*

We appreciate the opportunity to comment on the Preliminary FTC Staff Report "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers."

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, 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.

As an organization devoted to the development of standards that allow for global interoperability, we are convinced of the importance of requiring interoperability in the public policy domain.

The staff report does an admirable job of analyzing the evolution of consumer privacy protection. It also makes a commendable contribution to the development of a privacy framework appropriate to the 21st century. But, as the staff report acknowledges, there are important issues regarding the scope of the proposed framework and whether it applies only to data that can be "reasonably linked to a specific consumer, computer, or other device."

The staff report suggests that there are two categories of data: data that can be reasonably linked to a specific consumer, computer, or other device; and data that, while not currently linkable, may become so in the future. The report asks for comments regarding reliable methods for determining whether data is linkable or may become linkable.

If a party has unlimited time and unlimited resources, any data is *potentially* linkable. The staff report suggests that the framework apply only to data that could "reasonably be linked." But what would this actually mean? What would be "reasonable"? Would it be reasonable to make such linkage if any potential benefits are speculative or would not appear to justify the required effort to make the linkage now, or in the future? Would it be reasonable if the linkage would violate a firm's policies?

We applaud the staff's attempt to appropriately limit the scope of the framework. This is particularly important given that there are those who argue that because all data is potentially linkable, then all data should be subject to the framework.

We do not believe that sweeping all data into the framework would enhance privacy. We believe that sweeping in more data, virtually expanding the definition of personally identifiable

information to all information based on the *possibility* of linkage, would have unfortunate consequences. Rather than improving the protection of personal privacy, we believe that the approach of including all data would have the unwanted effect of resulting in less protection. Expanding the definition could well create disincentives for companies to minimize or avoid data linkages.

But while attempting to limit the scope to those situations where linkage would be reasonable, there is obviously considerable room for disagreement about the meaning of the phrase "reasonably be linked." Such ambiguity adds unwanted uncertainty to the framework.

Rather than basing the scope of the framework on whether data could reasonably be linked, we recommend that the scope of the framework be as follows: The framework applies to all commercial entities that collect or use consumer data that is linked to a specific consumer, or to a computer or device being treated as a proxy for a specific consumer.

We believe that the use of Privacy Impact Assessments (PIAs) can assist with defining and ensuring accountability with the Framework's scope. GS1 recently led the development of a Framework for a Privacy Impact Assessment 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*. This experience has convinced us that PIAs provide a useful tool in supporting the basic tenets of the proposed framework which we support: PIAs can help increase privacy awareness; build a privacy-enhancing culture throughout an organization; foster accountability; stimulate the adoption of privacy by design practices in the development of new products and services; and focus an organization's attention on the risks, if any, to privacy and the means to mitigate such risks.

The PIA is also a useful model to enable all the pillars of the FTC proposed Framework: transparency, choice and privacy by design. In practice PIAs can help firms determine when privacy issues arise and help them address those issues in a manner commensurate to the sensitivity of the data and the intended uses. PIAs can also help companies identify events that will trigger new reviews even after goods or services are deployed. PIAs foster informed decision making throughout the organization and promote accountability. For example if a firm does not intend to link data to a specific person, or a computer or device serving as a proxy for a person, the PIA process provides a mechanism to focus on the actions needed to prevent such linkages.

It is important to remember that the creation of PIAs are not without cost in time and resources. Small and medium-sized enterprises often do not have personnel dedicated to privacy protection, so the PIA process needs to reflect the resources and expertise available to small and medium- sized and their particular processes.

Because of the benefits that PIAs provide in support of the aims of the framework and the positive role that PIAs can play in developing effective self-regulation, we believe that companies should be encouraged to use them. One way to do this would be to allow companies to use PIAs to demonstrate that they exercised due care in regard to their practices and the goods and services that they offer. In order to foster candid self-analysis and to protect proprietary data and practices, we do not believe that there should be a requirement that PIAs be published as some have suggested. In addition, it is important to remember that different jurisdictions around the world may treat PIAs regarding the same globally offered good or service in multiple and conflicting fashions; this in is yet another reminder of the importance of achieving a globally interoperable privacy policy.

Another benefit of the framework and PIA process is that, appropriately constructed, it can provide great flexibility to accommodate new technologies and new collection and use of data. For instance, PIAs would be a useful tool to support the appropriate development of what has come to be known as the Internet of Things (IoT), the emerging technology through which objects can communicate with one another.

Among the components of the Internet of Things are mechanisms that allow for the identification of objects, such as RFID tags, as well as the potentially far more numerous autonomous or semi- autonomous sensors that in the future may number in the billions or even trillions. They are being used to monitor and control energy usage, collect climate data, detect radiation and biohazards, and even to safeguard our borders. These sensors will be gathering and transmitting a wide range of data which is potentially linkable to a specific consumer, or to a computer or device that serves as a proxy for a consumer, as we suggest to be the scope of the framework. Such technology raises important questions regarding under what circumstances privacy principles should apply, and, if so, how and when to appropriately apply privacy principles such as notice, choice, data access and other features. We believe the IoT has the potential to offer enormous benefits and we will need a flexible framework that can accommodate radical technological change and ever increasing complexity. PIAs may be a useful tool for this.

The staff report also points out the issues involved in anonymizing/de-identifying and re-identifying data. These issues, and in particular the related technical aspects, are exactly the kind of issues which the National Academy of Sciences could address. We recommend that the Academy be asked for its best judgment about the steps that firms should take to anonymize/de-identify data, recognizing that perfect and lasting de-identification is unlikely to be attainable. The Academy should be asked to make recommendations about the level of effort that would be reasonable for a firm to take to protect the anonymity of the data. If a firm followed the Academy's recommendations then, in any subsequent proceeding, it should be recognized as having exercised due care. The level of effort could, and should, be revisited over time as technology evolves, but a firm would know what it has to do to be in compliance with public policy requirements. This course of action would be similar to what the Commission has done in other areas in establishing best practices but would draw upon the technical expertise of the Academy. Alternatively the National Institute of Standards and Technology in the Department of Commerce could convene a broadly inclusive technical advisory process to establish standards for due care in anonymization/de-identification.

The staff report asks about the role of industry associations in educating businesses on consumer privacy. We strongly support these efforts. Beginning with its support for the AutoID Center at MIT and the development of the RFID standard known as the Electronic Product Code (EPC), GS1 has worked with its members to develop privacy protecting guidelines and practices when employing RFID tags to improve supply chain efficiency. From the earliest days of the introduction of bar codes, GS1 has realized that the success of its standards depends largely on consumer trust and we must work diligently to earn that trust. In addition to working with its membership on privacy protection, GS1 has worked with public policy makers to build globally interoperable privacy policies that mirror GS1's globally interoperable technology and business standards. We would encourage the Commission to examine what incentives might be available to encourage more of such activity by industry groups.

We would commend to the Commission that greater attention might be paid to the creation of positive incentives for the promotion of consumer privacy. Our members already have strong incentives to treat data appropriately if they are to keep the trust and respect of their customers. But there may well be other positive incentives such as the reduction of administrative burdens based on a firm's record of compliance or its having exceeded generally recognized privacy or security requirements. This is analogous to providing procurement incentives for builders or manufacturers who achieve increasing levels of sustainable construction or production. Similarly the Commission might consider the question of incentives when considering proposals on notice and consent. Providing standardized forms that communicate efficiently is important but a privacy promoting strategy would also include incentives for firms to continually improve their ability to communicate with those with other organizations and consumers.

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
www.DiscoverRFID.org
www.GS1US.org
www.GS1.org
www.EPCglobal.org
www.EPCglobalUS.org