

**Before the
Federal Trade Commission
Bureau of Consumer Protection
600 Pennsylvania Avenue, NW
Washington, DC 20580**

Regarding)
)
Federal Trade Commission (FTC))
(Bureau of Consumer Protection) Staff Report)
)
A Preliminary FTC Staff Report on)
"Protecting Consumer Privacy in an Era of)
Rapid Change: A Proposed Framework for)
Businesses and Policymakers")

**COMMENTS OF THE NATIONAL ASSOCIATION OF MANUFACTURERS
TO THE FEDERAL TRADE COMMISSION'S BUREAU OF CONSUMER
PROTECTION REGARDING THE PRELIMINARY FTC STAFF REPORT ON
"PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE:
A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS"**

The National Association of Manufacturers (NAM) is the nation's largest industrial trade association and represents manufacturers in every industrial sector and in all 50 states. The NAM is the voice of all manufacturing in the United States and informs policymakers about manufacturing's vital role in the U.S. economy. The NAM submits these comments in response to the preliminary staff report issued by the Federal Trade Commission (FTC) on December 1, 2010, "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers."

The relationship between manufacturers and the customers who entrust their data to them is based on industry's continuing efforts to protect the security, integrity and privacy of that data. Manufacturers recognize that respecting and safeguarding privacy builds consumer confidence in new and innovative technologies and services. To that end, industry's best practices in the proper handling of data are constantly adapting and evolving to address new threats. As technology applications and the use of the Internet continue to grow, both the government and the private sector are gathering more consumer information, including personally-identifiable information, to provide services. The increase in the collection and use of these data has raised public privacy concerns over what information is being collected and how the information is being used.

The preliminary staff report proposes a framework that promotes privacy, transparency, business innovation and consumer choice. We commend the FTC for taking on the important issue of consumer privacy and submit the following comments.

Companies Should Build Privacy Protections into Their Everyday Practices

Respecting consumer privacy is of utmost concern for NAM members, whom adopt and implement strict privacy policies based on industry best practices. The federal government has largely allowed industry self-regulation in the area of non-sensitive consumer privacy protection, and this effort has been successful. A number of online privacy seal programs have been established to help businesses develop the proper policies and practices that give consumers the confidence they need. These programs help educate businesses on how to develop meaningful privacy policies and practices and also promote strict compliance.

A good example of this best practice is the safe harbor established under the Children's Online Privacy Protection Act (COPPA) and the third-party seal programs created in COPPA's wake that help businesses comply with the Act. We believe these programs have been both successful and beneficial to industry and consumers, and they should be encouraged for widespread commercial sector use for all privacy applications.

The NAM supports an FTC-approved safe harbor framework that creates incentives for businesses to implement strong consumer privacy protections by subjecting them to an independent assessment of operator compliance. Modeled in part after the COPPA safe harbor, successful participation by companies in online privacy seal programs should provide them the ability to streamline their legal compliance, providing a presumption of compliance, allowing remedial action before sanctions are imposed and establishing a limitation on punitive and non-economic damages for both federal and state purposes.

Companies Should Simplify Privacy Choices for Consumers

The NAM believes that current industry practices are effective and that companies should make privacy notices available at all times. Company websites should provide customers with information about the organization's privacy policy both prior to and at the time of the collection of personally identifiable information.

The Definition of Personally Identifiable Information

Throughout U.S. commercial privacy law, the discussion of protecting consumer information is based on data that could be used to personally identify the consumer either on the network or physically. Personally Identifiable Information (PII) is information relating to a person who can be directly identified through a combination of one or more of the following factors:

- first name or first initial in combination with the last name;
- home or other physical address including street name;
- personal identification code in conjunction with a password required to access an identified account;
- Social Security number, tax identification number, driver's license number, passport number, or any other government-issued identification number;
- account balance, overdraft history, or payment history that personally identifies an owner or operator of a computer; or
- health or medical record.

The disclosure of any one factor by itself, or any factor in combination with publicly available, encrypted, obfuscated, disassociated, or aggregated information should not be considered PII.

The NAM recommends limiting the scope of PII to information that would reasonably lead to the personal identification of a specific consumer. This reduces the burden of compliance on data-collecting websites while providing consumers with equivalently strong privacy protection of information they would reasonably expect to be safeguarded.

A consumer should be defined as an individual acting in an individual, personal, or family capacity. In contrast, information such as name, title, business address and business telephone number should not be considered PII for individuals involved in business-to-business transactions, since it would unnecessarily interfere with reasonable business practices.

Small- and medium-sized data collectors – those who collect non-sensitive data from fewer than 5,000 individuals in any 12-month period – should be exempt from regulation. This will prevent the imposition of potentially onerous data handling requirements on entities that collect information incidentally to their business model.

Behavioral Advertising

The NAM believes a set of sound practices in the area of online behavioral advertising should apply to all online companies regardless of their technology or the platform used. The principles underlying these consumer protection practices are:

- **Consent**: The NAM believes that before a company captures certain Internet-usage data for targeted or customized advertising purposes, it should obtain meaningful affirmative consent from consumers. Such consent requires:
 - **Transparency**: There must be conspicuous, clearly explained disclosure to consumers as to what types of data are collected and for what purpose the data are being used, how that data are retained and for how long, and who is permitted access to the data.
 - **Affirmative Choice**: A consumer must provide affirmative consent before information can be collected and used for online behavioral advertising across multiple websites. A consumer's failure to provide consent should mean that there is no collection or use of that consumer's information for online behaviorally-targeted advertising based on tracking of the consumer's Internet usage across multiple websites.
 - **Consumer Control**: A consumer must have an ongoing opportunity to make a different choice about behavioral advertising. There must be clear and easy-to-use instructions to change preferences with regard to the collection of data for behaviorally-targeted advertising purposes.
- **Security**: Any company engaged in tracking and collecting consumers' online behavioral information must have appropriate access, security and technological controls to guard against unauthorized access to personal information.
- **Safeguards for Sensitive Information**: Special attention must be given to the protection of information of a sensitive nature (e.g., accessing medical websites). Specific policies may be necessary to deal with this type of information.
- **Certification**: Companies engaged in online behavioral advertising should agree to participate in a credible, third-party certification process to demonstrate to consumers that they are doing what they say with the information.

Companies Should Improve the Transparency of their Privacy Practices

Notice & Consent Issues

The NAM understands and appreciates the sensitivity many consumers have surrounding the surreptitious collection of their web browsing habits. The NAM supports providing notice to consumers when personal identifiable information is collected.

Any action taken by the FTC or Congress must not have unintended consequences for businesses that maintain multiple websites and require consumers to travel back and forth between different websites owned by the same business.

For example, a consumer may visit a car manufacturer's website that directs the consumer to a car dealership's website and then back to the manufacturer's co-branded but separate auto financing site. Or a consumer may visit a software manufacturer's website for a business application security patch, travel next to the gaming website for news on the latest releases and then travel again to the online store. All these websites may be co-branded but technically separate. For businesses with separate co-branded websites, collecting information on how consumers travel between their websites is critical to enhancing the customer's experience and ease of use.

Any notice and consent requirements should clarify that IP addresses are not covered information. Many websites collect the IP addresses of incoming visitors even before the webpage is delivered to the consumer's web browser. This is a situation that does not logically present itself as offering an opportunity to provide notice or an opportunity to consent. As noted above, an IP address by itself is not personally identifiable and presents no imminent privacy concerns to an individual if collected. A possible solution to this issue is to require a link to an electronic privacy notice (or via a link from an e-mail) once the page is fully served or when an e-mail is opened.

Third Party Exemption

NAM member companies often use service providers to help them reach out to customers and prospects with information on new products and services. A business that discloses PII to a service provider for purposes of executing these first-party transactions should be exempt from the consent requirements, as long as consent for collection was previously given and the service provider agrees to use the information solely to provide the agreed-upon service and does not disclose the information to anyone else.

While these relationships are governed by both contract and agency law, the FTC should account for instances where it is appropriate to indemnify a business from the actions of a service provider – such as when the service provider acts outside of the contractual relationship and without the knowledge or consent of the business.

The NAM appreciates the opportunity to share these comments and suggestions with the FTC as it finalizes its preliminary staff report, "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers." We thank you for considering our views and would be pleased to answer any questions you may have.

Respectfully submitted,

National Association of Manufacturers
1331 Pennsylvania Avenue, NW, Suite 600
Washington, DC 20004

Brian J. Raymond

Brian J. Raymond
Director, Technology and Domestic Economic Policy
braymond@nam.org
202-637-3000