Five Reasons Why U.S. Consumer NGOs Support a Strong EU Privacy Law

1. U.S. citizens/consumers lack comprehensive protection for their personal information under federal law and will benefit from a strong EU approach:
The European Union must act to help set a global standard protecting the fundamental right to privacy for citizens and consumers. The "self-regulatory" model endorsed by the Obama Administration and leading U.S. data collection companies has failed to protect consumers from having their information—including highly personal and sensitive data—being collected and used. Leading U.S. consumer groups have long endorsed the EU approach to creating a comprehensive legal framework for data protection. The attempt by the U.S. government and American companies to undermine current policies related to the proposed regulation is based on a fear that the EU will set a global standard requiring fair, transparent, and accountable data collection practices. The EU can help foster greater confidence in the marketplace by enacting rules that adequately protect consumer privacy.

Consumers in the U.S. face a formidable system of pervasive and real-time data collection across digital platforms. From PCs to mobile phones and apps to gaming devices, consumers have no meaningful capability to control what information can be collected or how it can be shared or used. Data on users' income, race/ethnicity, spending habits, content consumption, location, health, and presence of children are analyzed and used without their consent. Increasingly, online data is now merged with offline databases as well.

U.S. consumers currently have no national legislation protecting their data rights online. The Federal Trade Commission has only the power to make recommendations on policy; its new privacy framework provides no guarantee that consumers can actually have any control over their data. Nor has the Obama Administration's multistakeholder process, which began late last year, proved to be effective in defining how to protect consumer privacy. Other key multistakeholder initiatives favored by the U.S.—especially on Do Not Track at the W3C—have also foundered. The U.S. advertising industry's self-regulatory system, relying on icons for "opting-out," has been criticized by both policymakers and consumer advocates. While the Obama Administration's Privacy Bill of Rights called for new legislation, it has failed to produce any legislative framework. Comprehensive federal privacy legislation is unlikely, given the deadlock in Congress over many policy issues. While there have been a growing number of enforcement actions at the FTC, the agency is encumbered by a lack of resources. And although the FTC did subject both Facebook and Google to 20-year consent decrees, these agreements have so far failed to fundamentally improve how consumers control their information on these two leading platforms.

The work done by the EU on privacy, such as the initiatives of the Article 29 Working Party, has played a significant role strengthening U.S. policy proposals. For example, the FTC's December 2012 decision to declare that cookies, geo-location

data, and persistent identifiers are to be considered as "personally identifiable information" (PII) when used to commercially target children 12 and under online was greatly influenced by the EU's own work defining personal data. In Congress, a bi-partisan proposed law to expand the data protection of minors is based, in part, on the EU's current privacy proposal on the "right to be forgotten."

U.S. consumer NGOs have relied on the EU privacy framework and initiatives as a critical foundation for their own work with policymakers. The proposed comprehensive EU approach to protecting its citizens in the 21st century will enable consumer and privacy NGOs to advance how data can be protected outside the EU as well.

2. The growth of Big Data and the absence of privacy regulation threaten consumer welfare and undermine citizen rights.

Consumers increasingly rely on the Internet to engage in transactions related to their most personal decisions involving finance and health. From credit card and mortgage applications to searching for medical information and treatment, consumers now depend on the Internet to address issues of fundamental importance to their security and welfare. But in the U.S., information on a consumer's financial interests is largely unprotected online. Personal data can be collected, compiled, and shared by multiple parties to help determine credit, customer service, and other offers, without any requirement that consumers have access to their own information. "Predictive" data analytics make decisions about our credit or employment prospects, creating so-called "E-scores" that are used to evaluate an individual in real-time. Health marketers have access to consumer data revealing personal medical needs and interests. Sensitive data can be placed in an online profile and used to influence the kind of treatment one will be offered. The use of racial and ethnic information as part of online consumer profiling offers the potential to replicate the traditional discrimination historically found in the offline world, where the juxtaposition of race, income, and geography created forms of "redlining." Low-income and other "underbanked" consumers are already a target in the U.S. for so-called high-interest "payday " loan offers delivered via the Internet. Online data collection and profiling are also further fueling an avalanche of digital ads aimed at youth that promote the growing obesity epidemic. Consumers face further risk of their privacy as mobile phones increasingly morph into new forms of payment systems. Combined with the growth of geo-location technologies that instantly recognize both where and who we are (further integrating the physical and virtual world, and bringing one's personal geography more into the data collection equation), consumers now face a formidable, pervasive, and highly intelligent data collection infrastructure.

3. Threats to privacy are growing in the EU, especially from U.S. companies and techniques.

There is a dramatic expansion of data collection of online users, a digital "arms" race that is being fought in the U.S., EU, Asia Pacific, and other areas. Personal data are compiled and sold to the highest bidder in "milliseconds" via online auctions—all

without the knowledge or consent of the consumer. The U.S. online industry has pioneered the use of "ad exchanges" that automate the buying and selling of individuals—and which now has been exported throughout the EU. Leading U.S. companies have unleashed new forms of data collection practices that merge offline and online data, provide access to mobile and geo-locational information, and gather social media actions and behaviors of individuals and their friends. Increasingly, data are gathered from users across the multiple screens of PC's, mobile devices, and gaming platforms. Among the information combined for these ad exchanges on individuals are health, financial, racial, location and political interests. Since U.S. companies face few constraints on their data collection practices at home, they are constantly pushing to gather more user information in their products and services. By setting the global standard for the data collection industry, U.S. companies "push" these practices to their EU and global subsidiaries, partners, and industry associations.

4. U.S. consumers are concerned about their lack of privacy.
Polls and surveys from leading academics and consumer organizations reveal a U.S. public that wants to see their privacy protected online. A majority in a 2012 survey, for example, expressed concern about their mobile privacy, and how such personal details as address books and photos can be accessed. Nearly three-quarters of Americans do not want to be tracked online so they can be targeted for advertising, notes a 2009 University of Pennsylvania poll. A University of California at Berkeley survey found that younger users (18-24) are as strongly concerned about their privacy as older adults. Polls also indicate that U.S. users want greater limits on the amount of data that can be collected from them, and the ability for such information to be deleted at their request. Although there is overwhelming support for the passage of federal legislation protecting privacy in the U.S., because of industry opposition Congress has been unable to consider comprehensive privacy legislation.

5. Future growth of the online economy requires consumer confidence that their personal data will be protected.
Consumers are increasingly familiar with—and concerned about—their lack of basic data protection. The future growth of the digital economy depends on consumers feeling that their data—and their most personal transactions—are safe. Today, in the absence of regulatory safeguards, data collection "maximization" is the norm. Trust in the digital data system is challenged daily, as new forms of collection without user consent are revealed by the press. The industry is under siege because of its practices, and has to continually retool or launch new self-regulatory initiatives designed to calm policymakers and the public. Effective action from the EU setting a new standard for data protection will spur global public support for the digital economy. Such a EU policy will unleash greater growth for the online sector, foster innovation, and ensure citizens have meaningful rights in the Digital Era.

Prepared by Center for Digital Democracy and Consumer Federation of America