Statement of Jeff Chester, Executive Director

Center for Digital Democracy

Public Hearing before the Trade Policy Staff Committee on the

Transatlantic Trade and Investment Partnership (TTIP)

USTR

29 May 2013

The Center for Digital Democracy (CDD) urges the Obama Administration to negotiate a European Union (EU) and U.S. trade treaty that places the goals of ensuring consumer protection, civil liberties, and human rights alongside the interests of promoting job creation, investment, and innovation.[1] The USTR should not seek to include data protection in the TTIP and allow the distinct policy processes now underway in the U.S. and EU to evolve. Nor should policies addressing Digital Trade or "data flows" be used to undermine privacy and consumer protection frameworks and policies. There is no legitimate or fact-based basis to show that the U.S. and EU systems are complementary and should be subjected to an "interoperability" trade scheme.

Despite much-heated rhetoric from some in U.S. industry on "explicit and implicit barriers to doing business in and with Europe," U.S. companies can and should comply with EU rules designed to protect individual privacy rights. Indeed, U.S. online ad companies are doing financially quite well in the EU, despite their grumbling about having to comply with its data protection framework.

The USTR should also ensure meaningful transparency in the negotiating process, and facilitate the participation of consumer groups through the creation of a formal advisory body.

The current digital data collection landscape and its impact on privacy

[1] CDD is one of the country's leading independent NGO's focused on consumer protection in the digital era. It is a member of TACD.

Citizens and consumers on both sides of the Atlantic face an ever-growing threat to their privacy, as pervasive and primarily nontransparent digital data collection practices permeate nearly every aspect of our lives. Today, individuals are tracked, analyzed, profiled, and subjected to predictive analysis and real-time targeting techniques across key online platforms (including mobile and social media). Information harvested from consumers and citizens—about their finances, health status, ethnicity/race, their children, etc.—is increasingly subjected to data techniques that impact both their privacy and welfare.

CDD closely follows the U.S. online data collection industry, including its activities in the EU. U.S. digital marketing companies have exported data collection techniques to the EU, including the use of so-called programmatic buying services (ad exchanges) where individuals (without their knowledge) are auctioned off in milliseconds to the highest bidder, based on their ever-expanding data profiles. U.S. data collection companies have also acquired leading EU online ad firms and established a broad presence within the EU.[2]

The Administration must promote digital trade and related "data flows" in a responsible way that fully respects privacy and its critical role in democratic societies.

Both the EU and U.S. approaches to data protection are being re-examined and it is premature to address this issue in the TTIP

The EU's human rights-based approach to data protection is distinct from the U.S.'s principal focus on privacy as primarily a consumer-protection issue.[3] Unlike the U.S., which does not have a baseline privacy law, the EU has a long-established framework to empower its citizens regarding data protection. In the EU, as USTR knows, there are pending regulatory proposals that would revise its highly regarded data protection directive. The EU's revised privacy regulation could provide its citizens with greater control over the growing use of data profiling, which is expanding daily as a major threat to individual privacy.[4] The revised protections would also build upon the EU's already substantial regulatory oversight system for privacy, involving EU and national-based data-protection authorities.

In the U.S. there is only the potential promise of some form of national privacy law that might better protect consumer information, especially via digital media. The Obama

[2] For background on the role of U.S. companies and/or the data collection practices they have pioneered in the EU, see generally EMEA ExchangeWire, http://www.exchangewire.com/emea/ (viewed 28 May 2013).

[3] "Treaty of Lisbon: A Europe of Rights and Values," Europa, http://europa.eu/lisbon_treaty/glance/rights_values/ (viewed 28 May 2013).

[4] "Q&A on EU Data Protection Reform," European Parliament, 2 May 2013, http://www.europarl.europa.eu/news/en/pressroom/content/20130502BKG07917/html/QA-on-EU-data-protection-reform (viewed 28 May 2013).

Administration has not even released a draft of its promised legislation to implement its February 2012 Privacy Bill of Rights report.[5] It is doubtful that Congress will enact any new privacy legislation soon, especially given the opposition to any effective legislation by the powerful U.S. online data collection industry. (The same lobby opposed granting the Federal Trade Commission additional regulatory capabilities during the debate on the Dodd-Frank bill, so fearful was it of having a regulatory agency empowered to protect consumer privacy.)

Nor has the "multistakeholder" approach, endorsed by the Administration and favorably cited by a number of commenters in the USTR docket, been found to be a workable approach. Indeed, despite the endorsement of the White House, the FTC, and many congressional leaders, the more-than-two-year effort by the highly respected World Wide Web Consortium (WC3) to develop a "Do Not Track" technical standard is on the verge of foundering. U.S. online data companies on the WC3 "tracking protection" working group have been largely opposed to the adoption of any approach that would enable online users to make even a modest choice regarding the collection of their information by third-party data companies.[6]

The Administration's initial multistakeholder attempt to implement provisions of its Privacy Bill of Rights, now being conducted by the Department of Commerce, has involved nearly a year of debate over just one aspect of the many privacy issues that must be addressed under its proposed "Rights" (concerning a "short-form" privacy notice for mobile apps). Many consumer groups view the process as inadequate, and it remains to be seen whether the Commerce Department's multistakeholder initiative will continue in the near future with the participation of consumer and privacy NGOs.

Privacy is poorly protected in the U.S. and our regulatory system and enforcement efforts are inadequate

U.S. online companies are expanding daily the amount of data they collect on individuals, including on their networks of friends and others.[7] The FTC, Senate Commerce Committee Chairman Jay Rockefeller, the Bipartisan Congressional Privacy Caucus, and many other leading policymakers have raised concerns about the growing role data

[5] "We Can't Wait: Obama Administration Calls for A Consumer Privacy Bill of Rights for the Digital Age," The White House Blog, 23 Feb. 2012, http://www.whitehouse.gov/blog/2012/02/23/we-can-t-wait-obama-administration-calls-consumer-privacy-bill-rights-digital-age (viewed 28 May 2013).

[6] CDD is a member of the WC3's Tracking Protection working group.

[7] See, for example, "eXelate and Digiday Research Finds that Advertisers and Agencies Rank 3rd Party Online Data as the Most Essential Data Type for Audience Targeting on Both Direct Response and Branding Campaigns," 24 Apr. 2013, http://exelate.com/news/exelate-and-digiday-research-finds-that-advertisers-and-agencies-rank-3rd-party-online-data-as-the-most-essential-data-type-for-audience-targeting-on-both-direct-response-and-branding-campaigns/; PubMatic, "Demand More," http://www.pubmatic.com/demand-overview.php#targeting-audience-attributes (both viewed 28 May 2013).

brokers play in the collection and selling of consumer data in the U.S., especially online. (There is a GAO study underway on this issue, with a report expected). Social media data practices enable close surveillance of consumers on blogs, online video sites, and platforms such as Facebook. The location and geographic history of a consumer is increasingly collected, via mobile devices and related geo-location technologies, without meaningful consent. New ways to track and evaluate consumers for financial transactions have emerged, including so-called secret "e-scores." A major new trend is the real-time integration of online and offline data, especially related to consumer purchasing decisions.[8]

Some industry commenters suggest that the U.S.'s privacy framework is more robust than the EU's due to the FTC's enforcement work. Unfortunately, while the FTC's has made significant progress addressing privacy, it seriously lags in its ability to make meaningful changes to how a consumer's data are actually collected and used. Despite the privacy-related 20-year Consent Decrees imposed upon both Google and Facebook by the commission, designed to better protect online consumers regarding how their data, each company routinely engages in an almost daily expansion of how they collect and monetize user data. The FTC is only in the preliminary stages of addressing the serious threats to consumer privacy arising from social and mobile digital marketing. In addition, the only group of U.S. consumers who have any reasonable safeguards online for privacy is children under 13.[9] Once consumers turn 13 in the U.S., they are subjected to a vast array of data collection practices online. U.S. industry self-regulation of consumer privacy has also failed to stem the increasing pattern of personalized data collection and targeting across platforms.[10] Despite the claims of some commenters about the effectiveness of a "privacy compliance" regime in the U.S., the much-touted "privacy by design" framework is overshadowed by the "data maximization" approach to monetizing consumer information embraced by the commercial marketplace.

The EU's privacy system has been more capable of identifying consumer data protection issues at a much earlier stage, helping foster a more informed debate on how best to protect the rights of the public. The USTR should not accept claims that somehow because both regimes invoke the Fair Information Privacy Principles (FIPPS), there is sound basis to propose implementation of "interoperability" principles.[11]

---

[8] See, for example, Salesforce, "Introducing the Social Marketing Cloud," http://www.salesforce.com/socialmarketing/; Erica Ogg, "Flurry Opens Marketplace, a Real-time Bidding Ad Exchange for Mobile Apps," http://gigaom.com/2013/04/09/flurry-opens-marketplace-a-real-time-bidding-ad-exchange-for-mobile-apps/; Drawbridge, "Bridging Over 400M of Your Customers Across Devices," http://www.drawbrid.ge/ (all viewed 28 May 2013).

[9] CDD has been the leader on children's privacy, especially in connection with the passage and implementation of the 1998 Children's Online Privacy Protection Act (COPPA).

[10] Indeed, the current debate on implementing a Do Not Track system illustrates how the FTC and others view self-regulation as inadequate.

[11] Principally via its Article 29 Working Party: European Commission, "Article 29 Working Party," http://ec.europa.eu/justice/data-protection/article-29/ (viewed 28 May 2013).

The USTR should engage in fact finding to determine the impact on consumer privacy and welfare of proposals related to Digital Trade and Cross-border Data Flows before it takes action in these areas

While there is understandable interest to achieve agreement on the TTIP, USTR needs to review the impact of any proposal that would impact consumer protection. CDD believes, for example, that the "one-stop-shop" lead data protection regulator for U.S. multinational companies would adversely affect EU consumers and weaken overall privacy. In identifying potential areas for greater cooperation related to Digital Trade and e-commerce, the USTR should be guided by the facts. It should commission independent and objective reviews of the relevant marketplace and regulatory questions posed. Relevant and diverse stakeholders who have the issue expertise should review these analytical reports. Through such fact finding and stakeholder participation, the USTR will be in a better position to identify and pursue issues related to the digital marketplace

CDD also supports ensuring that nondiscrimination (network neutrality) is enshrined as a basic principle within the TTIP. As recommended by the Transatlantic Consumer Dialogue and other commentators, CDD respectfully requests that USTR make the TTIP negotiations transparent and open. All proposed drafts, texts, and other documentation should be available online. A formal advisory board composed of U.S. consumer and privacy NGOs should be created, to ensure that USTR is able to make decisions that reflect the highest standards of consumer protection. This is an especially critical perspective for USTR as it works on Digital Trade, e-commerce, and cross-border data flows.

CDD, as well as its consumer colleagues in the U.S. and TACD communities, stand ready to assist the USTR as it engages in the TTIP process.