Will the TTIP Create a “Made in America” Big Data Surveillance System?

Why the Transatlantic Trade and Investment Partnership (TTIP) Could Expand NSA and Other Governmental and Commercial Surveillance on Citizens

U.S. online marketing companies are pioneering the dramatic expansion of data collection throughout the world, as they gather, analyze, and make actionable all of our information. Giants such as Google and Facebook effectively become “private NSAs”—tracking us on social media, mobile devices, search engines, online games, and increasingly even when we are in the grocery or department store. Telephone companies involved with the NSA’s “bulk” data-collection program are expanding their own data gathering on the Internet and mobile devices as well. This information is used to create dossiers—online targeting profiles—on individuals. These personal digital records can reveal details on our financial status, health concerns, ethnicity/race, political interests, buying habits, and the technology we use. Through social and mobile data collection, these data-gathering companies even know our specific geographic location—and where we are likely to go—as well as whom we consider “friends” in our social networks. Our behaviors, interests, and background are continuously analyzed, identifying whether we should be targeted with ads and other commercial content connected to financial and health products, political campaigns, and more. Increasingly, offline information about us is being added—in real time—to our online profiles.

While U.S. online data companies will claim that all this information is used primarily for selling and interactive advertising, in reality it’s connected to a powerful system that uses personal data to make decisions about us in order to influence our behaviors. We are secretly “scored” by online data companies that use an ever-expanding array of “Big Data” techniques to determine content, product offers, prices, and customer service. Leading online companies, including Facebook, Google, AOL, Yahoo, and Microsoft, refuse to take responsibility for their role in establishing a global commercial surveillance infrastructure—placing the blame exclusively on the government—and not themselves. Instead, the U.S. data collection industry proudly proclaims to lawmakers and others that “data-driven marketing is a major export,” “a uniquely American creation,” and that commercial data targeting can be labeled accordingly: “Made in America.”

U.S. Internet companies have actively opposed new legislative proposals that would empower consumers to have more control over their online information. The data-marketing lobby has mounted fierce opposition to efforts to strengthen the EU’s data protection framework, fearing that such measures would cut the flow of data American
companies are now able to monetize with very little oversight. And now these companies want the Obama Administration to help them expand their ability to gather EU citizen information through the Transatlantic Trade and Investment Partnership (TTIP) trade agreement currently being negotiated in Washington and Brussels. Among the key goals of U.S. data companies and high-tech trade groups are removing any barriers to transatlantic E-commerce data flows and curtailing the EU’s more comprehensive approach to privacy. While the TTIP is said to promote jobs and economic growth, American companies view it as a political tool to evade the forward-thinking and history-based approach to privacy in Europe—where it is enshrined as a civil right. They are pressing the White House to craft a trade deal that enables U.S. businesses to collect data from Europeans more freely, without regard to the EU’s data and consumer protection rules. Under the guise of promoting “interoperability” and “regulatory convergence,” the U.S. industry groups are trying to strip away the ability of the EU to protect the public.

U.S. officials have made numerous trips to Europe claiming that the U.S. approach to protecting privacy is as robust as the EU’s—a claim that is not true, unfortunately. Online companies have no regulatory obstacles to their extensive collection and use of data on Americans. The Administration frequently points to the Federal Trade Commission’s recent 20-year agreements with Google and Facebook, in which the two companies promised to protect user privacy, as evidence of a robust protective framework. But despite these so-called “consent decrees,” the two digital behemoths expand their collection of data almost daily.

In fact, companies such as Facebook, Google, Yahoo, and others in the data targeting industry engage in many of the same tactics as the NSA. These companies have developed sophisticated and pervasive techniques to identify our locations, monitor our conversations, analyze our relationships and social networks, share our data with their partners, and use this personal information to make inferences and decisions about us (concerning our finances, health concerns, political interests, and the like). These companies frequently deny—as the NSA has—that they are invading our privacy. They purposely keep out of public view how they gather our information and make it “actionable” for marketing purposes. While the implications of state security and government secrecy profoundly affect our democratic way of life, so too does the private use of information by powerful private entities—especially those whose business models are designed to influence and shape our behavior and decision-making in the marketplace.

Here are a few examples of how the NSA and the U.S. commercial data industry share the same fundamental disregard for our privacy rights:

- **Spying on other countries**: NSA—operating throughout the world, including the EU. Google, Facebook, Yahoo—maintaining an extensive global data collection system in the EU, Asia Pacific, South America, and beyond.

- **Monitoring phone communications**: NSA—routinely collects phone records. Google and others—closely monitor mobile phone use, including our use of apps.
• **Tracking individual Internet users:** NSA—uses cookies and email and social media analysis to identify and track individuals. Google, Facebook and others—pioneered the expanding role of persistent identifiers such as cookies, along with social media analytic techniques to identify nodes of connected individuals. 

17

• **Using Big Data analytics:** NSA—employs advanced data analysis to identify patterns in terabytes of data. Google, Facebook, and many other companies—use Big Data processing and analysis for user tracking and targeting. 

18

• **Covert behavior:** NSA—engaged in secrecy about its data gathering. Online data companies—have also created an extensive collection system that is largely kept out of public view, with pinpoint tracking and targeting of individuals and the “customer’s journey” without consumers’ knowledge or consent. 

19

• **Ultimate goal:** NSA—to collect all information. US online companies, working with large data brokers—to do the same, in quest of a single view of an individual and all of that person’s connections. 

20

---


