



August 5, 2014

John Morris, Associate Administrator and Director of Internet Policy  
National Telecommunications and Information Administration  
U.S. Department of Commerce  
1401 Constitution Avenue, NW, Room 4725  
Attn: Privacy RFC2014  
Washington, DC 20230

The increasingly powerful role of Big Data in the expanding digital marketplace has reached a tipping point, ushering in a set of highly sophisticated, next-generation practices with far-reaching implications for consumer protection, privacy, and the health and well-being of Americans. The delay in offering even model legislation has contributed to the unchecked growth of unprecedented data gathering on Americans by commercial entities. The NTIA should make the following recommendations to the President:

- The Obama Administration should offer legislation that ensures its Consumer Privacy Bill of Rights framework actually provides individuals with the control over how their personal information is collected and used. Individuals should have the ability to make meaningful decisions about their information, regardless of whether it is collected by a social network, mobile operator, app network, financial institution, etc.
- Legislation should provide regulatory rulemaking authority to the Federal Trade Commission (FTC) on consumer privacy issues to develop these new rights. Legislation should require the FTC to conduct the necessary proceedings leading to a rulemaking within one year from the enactment of legislation. The same legislation should also call on agencies that currently have rulemaking authority, including the Consumer Financial Protection Bureau (CFPB), the Federal Communications Commission (FCC) and the Food and Drug Administration (FDA), to immediately initiate proceedings on consumer financial, telecommunications, and digital health privacy, respectively. Other agencies with sectorial authority on privacy issues not covered by the FTC and others should also be mandated to develop regulations.
- The current “multistakeholder” process convened by the NTIA should be replaced by the relevant agency rulemakings.

- The legislation should acknowledge the threats that much of Big Data-related collection pose to Americans today, and strongly state that it is in the best interests of the nation that businesses refrain from their current practice of ubiquitous data collection and profiling. It should accept that self-regulation has failed.
- The FTC, CFPB, FCC, and FDA should be mandated to report to the Nation, within six months after legislation is enacted, on how commercial Big Data practices are currently being used in ways that may be harmful to the public and not in the national interest. These reports should identify how current practices can discriminate against Americans, based on their race/ethnicity, sexual orientation, income status, age, residence, and other key variables.
- Based on these reports, the agencies will propose special regulatory safeguards as required to address sensitive data concerns.

While the Center for Digital Democracy (CDD) appreciates the work of the White House to raise the privacy issues connected to Big Data (Podesta report), we believe the Administration failed to adequately acknowledge the looming threat nearly every American currently faces from today's pervasive commercial data collection environment. All the data that are gathered about us today—from our use of mobile phones, gaming devices, PCs, Internet and cable television, loyalty cards, etc.—are flowing into the Big Data platforms either operated by, or affiliated with, leading U.S. corporations. Massive amounts of information are now processed in milliseconds, enabling real-time tracking and targeting of individual consumers wherever they are. A largely invisible network of companies collect and analyze data about an individual's behaviors, both online and off, to construct elaborate personal profiles tailored to that specific person. Increasingly, these digital dossiers are analyzed and scored, generating a report card on us that is used to determine how we are treated and considered in the marketplace. For example, our behaviors may lead to scoring that triggers offers to some of us for high-cost payday lending, expensive insurance, or unaffordable educational loans. This practice can generate marketing and related content that is harmful to the public health, especially to vulnerable individuals (including youth and the elderly). Big data practices enable companies to bypass or ignore certain individuals, offering special deals to some and higher prices to others, which raise troubling concerns about new forms of discrimination online.

The discriminatory practices found in today's Big Data system are not an aberration—but reflect the current business approach that has established the systematic use of our information as the norm. It reflects an unfortunate paradigm that the Obama Administration should challenge—that companies have the interest and right to gather and use our information so they can “manage” a person's identity. All of this occurs without the understanding, let alone the consent, of the individual. Big Data provides new opportunities for invisible interests to shape our

lives in a way that is profoundly undemocratic. Legislation should challenge these practices, making it clear that in America, individuals must be empowered to decide how their information is used in this era of predictive analytics and sophisticated, and largely nontransparent, methods that rely on data and digital media to influence their decisions.

For example, few Americans outside the U.S. digital data and targeting industry know they are the subject of real-time online “auctions,” in which they are sold to the highest bidder or preferred customer based on their demographic and behavioral profile. These “ad exchanges” are increasingly used to target multicultural Americans, especially Hispanics. Through the growing practice of hyper-local data collection, neighborhoods are being “sliced and diced” to enable marketers and others to precisely target both individuals and specific communities through their mobile devices. Stores are also being fitted with sensors and related devices that track and assess our every move. As our mobile devices further evolve to become digital wallets, even more of our most sensitive data will be exposed.

CDD has previously provided comments to both the White House and the NTIA on these issues. Today, it joins with a coalition of civil rights, consumer, and privacy groups calling for Big Data safeguards. It is time for the White House to act decisively on behalf of Americans and not be beholden to the Big Data lobby—which seeks to expand further what is nothing less than pervasive and ever-growing commercial surveillance.

Jeff Chester  
Executive Director  
Center for Digital Democracy