August 5, 2014

John Morris
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW.
Room 4725
Attn: Privacy RFC 2014
Washington, DC 20230
privacyrfc2014@ntia.doc.gov

Submitted through e-mail

Re: Big Data and Consumer Privacy in the Internet Economy, Docket No. 140514424–4424–01

Dear Mr. Morris:

On behalf of The Leadership Conference on Civil and Human Rights and the American Civil Liberties Union, we write to offer our comments in response to the National Telecommunications and Information Administration's (NTIA) Request for Public Comment. We urge the Obama administration to put forward a strong legislative proposal on consumer privacy and believe such a proposal should include language addressing the risks of discrimination that stem from new uses of data. [1]

As a threshold matter, we are pleased that the NTIA is considering issues of civil rights and discrimination in privacy legislation. As the White House stated in its May 2014 report *Big Data: Seizing Opportunities, Preserving Values*, "[a] significant finding of this report is that big data could enable new forms of discrimination and predatory practices." The report went on to observe that "[w]hether big data will build greater equality for all Americans or exacerbate existing inequalities depends entirely on how its technologies are applied in the years to come, what kinds of protections are present in the law, and how the law is enforced."[2] We look forward to working with the administration and with the NTIA to respond to these important observations with new policies that will protect privacy, combat discrimination, and support the use of data in positive ways that improve the lives of all people in the United States.

We outline below the importance of privacy for protecting civil rights, highlight the problem of data and discrimination, and outline three recommendations that would help address discrimination: (1) refine the multi-stakeholder process to address power differentials and the incentive for stalemate and delay; (2)

[1] For nearly 100 years, the ACLU has been our nation's guardian of liberty, working in courts, legislatures, and communities to defend and preserve the individual rights and liberties that the Constitution and the laws of the United States guarantee everyone in this country. The Leadership Conference is a coalition charged by its diverse membership of more than 200 national organizations to promote and protect the civil and human rights of all persons in the United States. The ACLU also supports specific privacy protections based on the FIPPs for any legislative proposal. Those are addressed in a separate joint filing with other consumer privacy organizations.
[2] Executive Office of the President, *Big Data: Seizing Opportunities, Preserving Values* at 53 (May 2014) (hereinafter *Big Data Report*).

revise the administration's Consumer Privacy Bill of Rights to address information beyond personally identifiable information; and (3) build technical competence in government.

Civil Rights Principles for the Era of Big Data

Both the ACLU and The Leadership Conference are signatories to *Civil Rights Principles for the Era of Big Data*, committing us to five key goals:

1. Stop High-Tech Profiling
2. Ensure Fairness in Automated Decisions
3. Preserve Constitutional Principles
4. Enhance Individual Control of Personal Information
5. Protect People from Inaccurate Data[3]

These principles are aimed at addressing the significant civil rights harms that can stem from the use of data. At the same time, several of these civil rights principles closely track the longstanding privacy frameworks of the Fair Information Practice Principles (FIPPs), which provide an important foundation for this administration's own Consumer Privacy Bill of Rights.

For example, stopping high tech profiling will mean giving consumers the right to exercise control over how information is collected from them and also respecting the context of that collection. Another area of broad overlap is protecting the accuracy of data. Here the Civil Rights Principles for the Era of Big Data were driven partly by a recognition that inaccuracies in databases can cause civil rights harms. Similarly, our principles recognize that control of personal information is crucial to protect the rights of vulnerable populations, including women, the formerly incarcerated, immigrants, religious minorities, the LGBT community, and young people.

Recognizing the overlap between privacy and civil rights enriches work in both areas. For privacy advocates, it resoundingly rebuts the canard that privacy violations do not harm anyone or that if you have nothing to hide, you have nothing to worry about. For civil rights leaders, it helps identify the pernicious and subtle discrimination that can pervade new systems, and helps pave the way for a high-tech civil rights enforcement agenda.

The Problem of Data and Discrimination

In some instances, new uses of data have already worsened existing inequality. Big data has the potential to exacerbate that further. The *Big Data Report* recognized this, noting that "big data technologies can cause societal harms . . . such as discrimination against individuals and groups. This discrimination can be the inadvertent outcome of the way big data technologies are structured and used. It can also be the result of intent to prey on vulnerable classes."[4]

As the *Big Data Report* notes (and as the ACLU has long highlighted), the E-Verify program illustrates one very serious example of this type of discrimination. E-Verify is the voluntary, government-run system that employers can use to check whether new employees are work eligible. According to

[3] For a full description of the principles, please see: "Civil and Human Rights Orgs Speak Out for the First Time on Privacy and Big Data Policy," Feb. 27, 2014. Available at: http://www.civilrights.org/press/2014/civil-human-rights-orgs-speak-out-on-big-data-privacy.html

[4] *Big Data Report* at 51.

government reports, this system has an error rate that is 20 times higher for foreign-born workers than for those born in the US.[5]

This experience provides an important lesson for commercial systems. E-Verify has been under development since first authorized in 1996, uses data only from one fairly homogenous source—the governments—and is frequently audited. Yet after nearly 20 years, persistent errors remain. That strongly suggests that existing commercial systems, which are fairly new and untested, use data from widely different sources, and operate with no transparency, could be even more flawed. The consequences of errors in these commercial systems are growing and can be severe, including wrongly labeling individuals as engaged in fraud or as meriting additional scrutiny before they can gain access to fundamental financial services like bank accounts.[6]

In another example highlighting the intersection of consumer privacy and discrimination, a major auto insurer has begun to deny its best rates to those who often drive late at night, such as those working the night shift. The insurer knows each driver's habits from a monitoring device, which drivers must install in order to seek the insurer's lowest rate.[7] Unfortunately, this type of rate discrimination ignores the racial disparities of individuals working late shifts. While this type of data driven discrimination may have an actuarially sound basis – perhaps because it includes a higher mix of drunk drivers – the fact is that it will result in a clear racial bias.

Big data can also be used to target vulnerable populations and thus facilitate predatory marketing directed toward such groups as seniors or people with physical and mental disabilities. Unscrupulous companies can find vulnerable customers through a new industry of highly targeted marketing lists, such as one list of 4.7 million “Suffering Seniors" who have cancer or Alzheimer’s disease.[8] Some advertisers boast that they use web monitoring technologies to send targeted advertisements to people with bipolar disorder, overactive bladder, and anxiety.[9]

There is also potential for more direct forms of discrimination. A recent report by the Federal Trade Commission (FTC) highlights the disturbing practice of data appending.[10] Using massive databases of consumer information, data brokers can take many types of consumer personal information, such as an email address, and append many other types of information about that consumer, such as race, religious affiliation, ethnicity, gender, and age. As FTC Commissioner Julie Brill notes in her statement accompanying the report:

> Nothing in the Commission’s report suggests that data brokers or their clients are running afoul of anti-discrimination laws. It is foreseeable, however, that data that closely follow categories that are not permissible grounds for treating consumers differently in a broad array of commercial transactions will be used in exactly this way.[11]

---

[5] Government Accountability Office, *Federal Agencies Have Taken Steps to Improve E-Verify, but Significant Challenges Remain*, at 40 (2010) available at: http://www.gao.gov/products/GAO-11-146

[6] Federal Trade Commission, *Data Brokers: A Call for Transparency and Accountability* at 48 (May 2014) (hereinafter *Data Brokers*).

[7] David Robinson, As Insurers Embrace Big Data, Fewer Risks Will Be Shared, Equal Future (Nov. 20, 2013); Kim Gittleson, How Big Data is Changing the Cost of Insurance, BBC (Nov. 14, 2013); The Economist, How’s My Driving? Gizmos that Track Driving Habits Are Changing the Face of Car Insurance (Feb. 23, 2013); Clint Boulton, Auto Insurers Bank on Big Data to Drive New Business, Wall Street Journal CIO Report (Feb. 20, 2013).

[8] Senate Commerce Committee majority staff, *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes* (2013).

[9] Julia Angwin, “The Web’s New Gold Mine: Your Secrets,” *Wall Street Journal* (July 30, 2010).

[10] FTC, *Data Brokers* at 24.

[11] Concurrence of FTC Commissioner Julie Brill, *Data Brokers* at C-1.

Such a clear potential for discrimination must be addressed in order to effectuate a meaningful Consumer Privacy Bill of Rights.

Potential Solutions for Data Driven Discrimination

While the FIPPs remain highly salient in the world of big data analytics, and the current evidence indicates a clear potential for improper and illegal discrimination through the use of big data, several steps would improve the administration's approach to protecting privacy with respect to civil rights even as we evaluate what is clearly a nascent field of study.

Refine the Multi-Stakeholder Process

The White House Privacy Blueprint, released in 2012,[12] outlined a consumer bill of rights and a mechanism to implement those rights, relying in significant part on a multi-stakeholder process.[13] While a multi-stakeholder process offers some important benefits, such a process has serious limitations when it comes to the protection of civil rights. The most important deficiency is the significant "asymmetry of power" and resources between organizations and companies benefitting from more widespread use of big data and the organizations that possess the most expertise on civil rights protections.[14]

For example, the first multi-stakeholder process undertaken by the NTIA addressed mobile application transparency.[15] A glance at the summary of meetings, briefings and draft policies is sufficient to demonstrate the high intensity of resources dedicated to just one such process.[16] Over the course of about one year, there were 16 formal meetings, at least six stakeholder briefings, 17 written comments, and approximately 18 drafts of a code of conduct. By the end of the process, 16 outstanding issues remained, narrowed from an original 30.[17] The ACLU was an active participant in this process and worked hard to craft a solution that benefits consumers. However, we believe that any participant in this process would describe it as extremely labor intensive and cumbersome. The ACLU certainly found it to be so.

Participating in such a process requires significant resources, much of it specialized and highly technical. The resources and expertise of affected industry sector groups will virtually always outpace the capacity of civil rights organizations, creating uncertainty regarding the ability of the process to protect the needs and concerns of the civil rights community.

To rectify this imbalance, we recommend that a public advocate within the administration be appointed to augment the analysis and consideration of civil rights concerns within the multi-stakeholder process. If the government funded and resourced such a role, it could help to ameliorate the disparities in process that might otherwise undermine the validity of the multi-stakeholder dynamic.

---

[12] *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (White House, February 2012). The process would engage companies and consumer representatives to produce a code of conduct. Companies that adhere to such a code would receive favorable consideration by the Federal Trade Commission in enforcement proceedings, and under legislation might offer a legal safe harbor for conduct. *Consumer Data Privacy* at 24.
[13] *Consumer Data Privacy* at 23.
[14] *Big Data Report* at 3.
[15] NTIA, Privacy Multistakeholder Process: Mobile Application Transparency, http://www.ntia.doc.gov/other-publication/2013/privacy-multistakeholder-process-mobile-application-transparency
[16] See Privacy Multistakeholder Process: Previous Meeting Information, available at: http://www.ntia.doc.gov/other-publication/2013/privacy-multistakeholder-process-previous-meeting-information
[17] *Id.*

The current process also lacks a mechanism to push compromise when inaction may benefit some parties. NTIA's role, as explained in the Privacy Blueprint, is to "help the parties reach clarity on what their positions are and whether there are options for compromise toward consensus, rather than substituting its own judgment." The Blueprint acknowledges that the most difficult issues might be resolved later in the process and suggests that multi-stakeholder parties should set out rules or procedures to "reach an orderly conclusion, even if there is not complete agreement on results."[18]

Within the multi-stakeholder process, however, there is no mechanism to effectuate a code of conduct if it is not accepted by the companies it is intended to regulate. If the behavior that is being governed violates longstanding civil rights, such an outcome would be untenable. In such a sensitive area, where some companies may be loath to admit they have potentially engaged in discrimination, and where others may be deliberately using data to target vulnerable populations, government action or judgment is necessary to avoid stalemate and delay. In order to ensure that the process is not indefinitely stalled by a lack of consensus regarding civil rights protections, the Federal Trade Commission, in consultation with the public advocate, should be given the authority to act as the final arbiter of disputes. Such a process could operate in a similar manner to a negotiated rulemaking.[19]

Move Beyond Personally Identifiable Information

As the *Big Data Report* explains, personally identifiable information (PII) is not the only type of information that can lead to civil rights violations and harm, particularly in the era of big data. Accordingly, the Consumer Privacy Bill of Rights should be revised to acknowledge information and data beyond PII.

By its terms, the Consumer Privacy Bill of Rights "applies to commercial uses of personal data. This term refers to any data, including aggregations of data, which is linkable to a specific individual."[20] The *Big Data Report* outlines the history of redlining in lending, explaining that mortgage lenders in the early 20th Century would use location data to make assumptions about individuals, assuming for example that certain neighborhoods were home to particular racial or ethnic groups, and would use geography as a proxy to discriminate against African-Americans, Latinos, Asians and Jews.[21] "Just as neighborhoods can serve as a proxy for racial or ethnic identity, there are new worries that big data technologies could be used to 'digitally redline' unwanted groups, either as customers, employees, tenants, or recipients of credit."[22]

For example, a person could be denied credit because big data analytics conclude he or she shares characteristics with "unwanted groups," without ever being personally identified within the meaning of PII or the Consumer Privacy Bill of Rights. A Bill of Rights that ignores the harms that members of groups or communities suffer will fail to address a broad range of significant harms. The Consumer Privacy Bill of Rights should acknowledge that individuals can suffer serious harms even when they are not individually identified, and should permit protections that extend to membership in groups.

[18] *Consumer Data Privacy* at 27.
[19] *See* 5 USC § 561 *et seq*.
[20] *Consumer Data Privacy* at 10. The Blueprint notes that this definition is similar to the government's definition of "personally identifiable information." *Id*. at note 12. Personally Identifiable Information refers to information "that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual." *Id*.
[21] *Big Data Report* at 53.
[22] *Id*.

Build Technical Competence in Government

We strongly endorse the White House's recommendation that:

> [t]he federal government's lead civil rights and consumer protection agencies … expand their technical expertise to be able to identify practices and outcomes facilitated by big data analytics that have a discriminatory impact on protected classes and develop a plan for investigating and resolving violations of law in such cases.[23]

As the report highlighted, "the same algorithmic and data mining technologies that enable discrimination could also help groups enforce their rights by identifying and empirically confirming instances of discrimination and characterizing the harms they caused."[24] Yet in a cutting edge and technology-driven field, the expertise to use big data to further civil rights is scarce.

Accordingly, we urge the administration to recruit experts in big data techniques to work in civil rights and consumer protection governmental agencies. The administration should prioritize budget allocations for these positions. As agencies develop their plans to implement this recommendation, we encourage them to include civil rights and privacy advocates. Moreover, funding programs or other incentives to promote additional education or training by veteran civil rights attorneys within the government in big data analytics would promote the positive uses of big data and further enhance the government's expertise in this area outside of the intelligence community. With adequate funding, collaborative work between civil rights organizations and such experts could reinforce these gains in the non-profit sector. Programs that educated non-governmental advocates would be a welcome complement. Finally, the Administration should consider the establishment of a federal advisory committee with particular technical expertise in both big data and discrimination.[25]

As its contribution to this area, the civil rights community is developing mechanisms to increase its own technical competence, as well as to develop scholarship and research regarding the intersection of big data analytics and civil rights. This fall, civil rights leaders and researchers will host a major conference to better understand the intersection of big data, civil rights, and discrimination. The administration should participate in, support, and augment this type of effort.

In the coming years, the use of data will have a greater and greater impact on the lives of all Americans. In order to assure that big data serves the best interest of each of us civil rights must be a key part of any privacy framework. The Leadership Conference and the ACLU look forward to continuing to work with the Obama administration to make that aspiration into a reality. If you have any questions about these comments, please contact Corrine Yu, Leadership Conference Managing Policy Director, at 202-466-5670 or yu@civilrights.org or Chris Calabrese, Legislative Counsel, American Civil Liberties Union, at 202-715-0839 or ccalabrese@aclu.org.

Sincerely,

The Leadership Conference on Civil and Human Rights
American Civil Liberties Union

---

[23] *Id.* at 65.
[24] *Id.* at 53.
[25] 5 USC Title 5, Appendix II.