Civil Rights Principles for the Era of Big Data

February 2014

Technological progress should bring greater safety, economic opportunity, and convenience to everyone. And the collection of new types of data is essential for documenting persistent inequality and discrimination. At the same time, as new technologies allow companies and government to gain greater insight into our lives, it is vitally important that these technologies be designed and used in ways that respect the values of equal opportunity and equal justice. We aim to:

1. **Stop High-Tech Profiling**. New surveillance tools and data gathering techniques that can assemble detailed information about any person or group create a heightened risk of profiling and discrimination. Clear limitations and robust audit mechanisms are necessary to make sure that if these tools are used it is in a responsible and equitable way.
2. **Ensure Fairness in Automated Decisions**. Computerized decisionmaking in areas such as employment, health, education, and lending must be judged by its impact on real people, must operate fairly for all communities, and in particular must protect the interests of those that are disadvantaged or that have historically been the subject of discrimination. Systems that are blind to the preexisting disparities faced by such communities can easily reach decisions that reinforce existing inequities. Independent review and other remedies may be necessary to assure that a system works fairly.
3. **Preserve Constitutional Principles**. Search warrants and other independent oversight of law enforcement are particularly important for communities of color and for religious and ethnic minorities, who often face disproportionate scrutiny. Government databases must not be allowed to undermine core legal protections, including those of privacy and freedom of association.
4. **Enhance Individual Control of Personal Information**. Personal information that is known to a corporation — such as the moment-to-moment record of a person's movements or communications — can easily be used by companies and the government against vulnerable populations, including women, the formerly incarcerated, immigrants, religious minorities, the LGBT community, and young people. Individuals should have meaningful, flexible control over how a corporation gathers data from them, and how it uses and shares that data. Non-public information should not be disclosed to the government without judicial process.
5. **Protect People from Inaccurate Data**. Government and corporate databases must allow everyone — including the urban and rural poor, people with disabilities, seniors, and people who lack access to the Internet — to appropriately ensure the accuracy of personal information that is used to make important decisions about them. This requires disclosure of the underlying data, and the right to correct it when inaccurate.

Signatories:

American Civil Liberties Union
Asian Americans Advancing Justice — AAJC
Center for Media Justice
ColorOfChange
Common Cause
Free Press
The Leadership Conference on Civil and Human Rights
NAACP
National Council of La Raza
National Hispanic Media Coalition
National Urban League
NOW Foundation
New America Foundation's Open Technology Institute
Public Knowledge

Civil Rights and Big Data: Background Material

High-Tech Profiling

- The FBI has recently engaged in a racial and ethnic mapping program that uses crass racial and ethnic stereotypes to map American communities by race and ethnicity for intelligence purposes.
- Police in New York used license plate readers to record all the cars visiting certain mosques, allowing their movements to be tracked later. New technology made this surveillance cheap enough that it could happen without a clear policy mandate.
- Law enforcement can use new social media monitoring tools to investigate nearly anyone at low cost. These systems need audit records and usage rules to ensure they are used fairly.

Automated Decisions

- Financial institutions can now gather detailed information on trivial consumer missteps, such as a one-time overdraft, and use it to bar customers from opening bank accounts.
- 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.

Constitutional Principles

- Information from warrantless NSA surveillance has been used by other federal agencies, including the DEA and the IRS — even though it was gathered outside the rules that normally bind those agencies.
- Databases like the so called “no fly” list are used to bar US citizens and legal residents from flying, without a fair process for reviewing these determinations.
- People who have access to government databases have often used them for improper purposes, including to leak confidential information about public figures and to review without reason the most intimate communications of strangers.

Individual Control of Personal Information

- New financial startups are using social network data and other "digital traces" to microtarget financial products. They claim to act outside the scope of existing consumer protections against unfair lending practices.
- 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.
- Some advertisers boast that they use web monitoring technologies to send targeted advertisements to people with bipolar disorder, overactive bladder, and anxiety.
- Location-aware social media tools have allowed abusive spouses and partners to learn the whereabouts of their victims in real time.

Risks of Inaccurate Data

- Government employment verification systems such as E-Verify demonstrate a persistently higher error rate for legal immigrants, married women, naturalized citizens, and individuals with multiple surnames (including many Hispanics) than for other legal workers, creating unjustified barriers to employment.
- Background check companies frequently provide inaccurate information on job candidates that stops them from being hired. While under law individuals are supposed to be able to correct these errors, they frequently recur and employers are not required to re-hire victims of misidentification.
- People often lose job opportunities due to criminal history information that is inaccurate, or that has nominally been expunged.