February 17, 2011

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: A Preliminary FTC Staff Report on "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers."

In response to the Federal Trade Commission's ("FTC") *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*, the Constitution Project submits these comments regarding data collection and use in the private sector.

The Constitution Project (TCP) is a nonprofit organization in Washington, DC that promotes and defends constitutional safeguards by bringing together liberals and conservatives who share a common concern about preserving civil liberties. The Constitution Project's bipartisan Liberty and Security Committee, launched in the aftermath of September 11th, brings together members of the law enforcement community, legal academics, former government officials, and advocates from across the political spectrum who develop and advance proposals to protect civil liberties as well as our nation's security.

As part of this work, the Constitution Project's Liberty and Security Committee has released a report entitled *Principles of Government Data Mining: Preserving Civil Liberties in the Information Age*.[1] This report urges the government to adopt policy reforms to ensure that we protect individuals' privacy interests and proposes specific recommendations for measures to incorporate safeguards into government data mining programs while preserving their benefits.

The report provides background on the federal government's expanded reliance on data mining, which the report defines as any use of computing technology to examine large amounts of data to reveal relationships, classifications, or patterns. These programs employ thousands of databases and hundreds of applications to mine law enforcement, communications, and intelligence data for criminal, terrorist, or national security threats. The report examines the data collection stage as well as the actual programs that mine the data. While TCP's report recognizes that data mining can offer significant benefits, it also outlines the potential for such programs to encroach on privacy rights and civil liberties. To combat these concerns, it recommends, among other proposals, that the government should establish and use a comprehensive data mining plan governing scope and intended uses, that agencies responsible for data mining perform regular internal evaluations of each program's effectiveness and costs, and that the government provide

[1] An electronic copy of *Principles for Government Data Mining: Preserving Civil Liberties in the Information Age* can be found at the Constitution Project's website, at http://www.constitutionproject.org/pdf/DataMiningPublication.pdf

comprehensive accountability and oversight to prevent overreach and allow for substantive redress.

While the Constitution Project's report focuses on government data mining, TCP's Liberty and Security Committee explicitly noted that data mining by private companies implicates similar privacy concerns, and therefore recommended extending these principles to the private sector. The report states that: "Although private data mining is beyond the scope of this report, it still implicates similar privacy concerns and therefore we recommend that federal, state, and local governments contemplate private-industry regulation or oversight to protect individual liberty interests."[2] TCP's recommendations for incorporating safeguards into the data collection stage and for regulating the government's use of personal information may be easily applied to the context of the FTC's inquiry into data practices by private companies.

Therefore, the Constitution Project commends the FTC's initiative in releasing a proposed framework, and urges the agency to expand upon its proposal as outlined below. As set forth below in more detail, the Constitution Project supports several of the features in the FTC's proposal which are consistent with TCP's own report, and suggests additional measures to be included in the FTC's final framework. The FTC proposed numerous specific questions in its proposed framework. Many of the FTC's questions are beyond the scope of TCP's data mining report and the issues addressed by TCP's Liberty and Security Committee. However, TCP's comments below address the FTC's questions regarding data retention, data minimization, notice, and transparency of data practices.

Positive Aspects of the FTC Proposal

Many of the FTC's suggestions are broadly consistent with the Constitution Project's report, and TCP urges the FTC to implement these recommendations as described below. Overall, TCP applauds the FTC's dual focus on the need for companies to incorporate privacy protections throughout their operations and on the importance of increasing the transparency of data practices.

In general, just as there are beneficial uses for data mining in the governmental context, there are also legitimate and beneficial uses for corporate data mining. However, it is critical that proper privacy safeguards be incorporated into any program collecting and storing personal data from individuals. Similarly, as the FTC report urges, companies should increase transparency of their data practices, and the Constitution Project agrees that users should be provided with meaningful choice regarding the extent of the data they share and the parties to whom the data are ultimately transmitted.

[2] The Constitution Project, *Principles for Government Data Mining: Preserving Civil Liberties in the Information Age* 9 n.* (2010).

The FTC's emphasis on maximizing data accuracy and limiting data retention is well-placed. The Constitution Project endorsed both principles in its recommendations for government data mining, and the same need for safeguards applies with equal force in the private sector. TCP welcomes the FTC's recommendation that companies should retain consumer data "for only as long as they have a specific and legitimate business need to do so,"[3] which parallels TCP's recommendation that government agencies should set retention periods at the "minimum duration required to accomplish the operational purposes" of the program.[4] The longer data are stored, the higher the chance that they will be misused or that individuals without authorization gain access to the data.[5] It may be appropriate to vary retention periods depending on the sensitivity of the data and the use to which the company is putting it. Mass, long-term storage of personally identifying information ("PII") presents an attractive target for abuse and creates a serious risk of misuse. At the expiration of retention periods, all traces of the data should be deleted, including from logs, buffers, and other locations.[6]

The FTC should also continue to focus on the elements of its framework that emphasize data minimization.[7] The FTC's recommendation that "companies should collect only the information needed to fulfill a specific, legitimate business need,"[8] is consistent with TCP's recommendation that government agencies "should carefully design programs to minimize acquisition of extraneous data unrelated to the program's purpose."[9] In the current landscape, once corporations have begun to collect and retain data, there are few, if any, incentives to limit the type and scope of data which they obtain, even if the data bear little or no relationship to expressed business purposes. Companies may seek to gather additional data based on the assumption either that the data may be useful at some later point, or that the data can be sold to a third-party data provider. Given the risks of abuse and misuse from storing vast quantities of data, companies should be required to adopt clear rationales for the original data collection,[10] in addition to a requirement that, once collected, data are stored securely with appropriate anonymization techniques to ensure that any security breaches cause minimal damage.

---

[3] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change* 46 (2010).

[4] The Constitution Project, *Principles for Government Data Mining: Preserving Civil Liberties in the Information Age* 27 (2010).

[5] *Id.*

[6] *Id.*

[7] *Id.* at 26-27.

[8] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change* 45-46 (2010).

[9] The Constitution Project, *Principles for Government Data Mining: Preserving Civil Liberties in the Information Age* 27 (2010).

[10] *Id.* at 20 (outlining a similar government requirement that data be mined only for specific, clearly articulated purposes pursuant to an established plan).

TCP applauds the FTC's recommendation that companies employ physical, technical, and administrative safeguards to protect data.[11] Specifically, TCP firmly believes that the FTC should make every effort to act on its proposal to make "use of privacy-enhancing technologies to establish and maintain strong privacy policies."[12] TCP's data mining report recommends similar safeguards, and encourages the use of technical measures, such as data encryption, as well as contractual terms to provide legal guarantees.[13] These safeguards can provide both peace of mind and protection for individuals whose data has been collected as well as allow recourse against private companies who have mishandled the data. Further, the FTC proposes, and TCP supports, the idea that these safeguards should be developed up-front through a privacy policy that is both comprehensive and appropriate for the individual company (e.g., smaller companies dealing with less data collection need not have privacy policies that are as detailed and fully developed as larger, more data intensive companies).[14] TCP has long advocated the early adoption of privacy policies, so that these policies are in place before the covered program is implemented.[15]

Recommendations for Additions and Changes to the FTC Proposal

While the FTC's report focuses on several important themes and outlines many specific, laudable methods, the FTC's final framework should also cover issues not currently addressed and expand upon other suggestions given only cursory treatment. Specifically, the FTC should provide a framework for redress and accountability in greater detail, analyze issues associated with user notice and consent before mined data are turned over to other parties, especially the government, and include a more complete discussion of the government's role in enforcement.

The FTC's proposed framework's focus on data accuracy and sound retention policies is commendable. However, the proposed framework gives only cursory treatment to the need for a process that can provide redress for users and accountability for corporations.[16] Improper use of data can expose users to significant harm, so it is

[11] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change* 44-45 (2010).

[12] *Id.* at 52.

[13] The Constitution Project, *Principles for Government Data Mining: Preserving Civil Liberties in the Information Age* 27 (2010).

[14] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change* 49 (2010).

[15] The Constitution Project, *Guidelines for Public Video Surveillance: A Guide to Protecting Communities and Preserving Civil Liberties* 34 (2006) (encouraging communities to establish rules for the collection and storage of video surveillance data to protect the rights of identifiable individuals captured by video surveillance programs).

[16] The Constitution Project, *Principles for Government Data Mining: Preserving Civil Liberties in the Information Age* 23 (2010) (recommending a system of redress and appeal for individuals who are harmed by government data mining programs).

important that the FTC emphasize both enforcement mechanisms by the government to ensure corporate compliance and describe the avenues open to individuals whose data have been misused and who seek meaningful redress opportunities. The FTC report asks whether consumers should be given the opportunity to view and correct personal information about themselves held by a company. As TCP recommends in the context of government programs, whenever feasible, individuals should have the opportunity to review data on file about them and correct any misinformation.[17] Individuals have the most incentive to safeguard their personal data. Therefore, providing users with the tools necessary to monitor the data's accuracy greatly increases the chances that all data are accurate, reliable, and complete.

As the FTC's report indicates, corporations frequently turn data they have collected over to third parties. These third parties could be, in some cases, large data brokerage houses or, in other cases, the government. When data are transmitted to another party, the user should in most cases have the opportunity to consent to the transfer. In cases where the consent has already been obtained or, as in the case of government mandated transfer to one of its agencies, no consent is required, users should be given notice.[18] Without notice, users will not be able to maintain control of their data since any number of parties could gain access to the data without any knowledge of the transfer on the part of the user.[19]

The Constitution Project fully supports the concept that non-consumer facing companies, such as third-party data brokerage centers, should be required to develop a standardized method to provide users access to data about them so that they can participate in the management and accuracy of the data.[20] However, to the extent that any such mandate would involve government supervision and therefore government access to the data itself, the final framework should incorporate careful protections to limit governmental uses of the data for other programs. Otherwise, involving the government as a supervising entity may risk further exposure of users' private data. When the government does gain custody of an individual's data and takes any action or makes a classification of an individual because of that data, the individual should be notified.[21] Additionally, when they are acting as government contractors, private

---

[17] *Id.* at 24.

[18] *Id.* at 22 (advocating for a comprehensive contemporaneous and delayed notification system).

[19] TCP's data mining report notes that in the case of governmental data mining efforts, there may be some cases where contemporaneous notice is not possible due to concerns over ongoing criminal activity or for national security reasons. In these cases, a system of delayed notice should be established. *See id.* However, these concerns will not typically apply in the context of consumer data held by private companies.

[20] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change* at 63.

[21] The Constitution Project, *Principles for Government Data Mining: Preserving Civil Liberties in the Information Age* 22 (2010).

companies should be required to follow all data mining rules and principles which apply to the government.[22]

Establishing a framework for private industry data mining is essential to protect the privacy interests of online consumers. The fact that many companies use PII for purposes that the user has no knowledge of and that significant data breaches by private companies have been documented[23] only underscores the extent of the problem and the need to incorporate proper safeguards. The FTC's proposed framework is an important first step in establishing a comprehensive system that can benefit both individual users and the online community at large. The Constitution Project encourages the FTC to revise and push forward with its efforts to achieve substantive change, taking into consideration these comments.

Sharon Bradford Franklin
Senior Counsel
The Constitution Project
1200 18th Street, NW
Suite 1000
Washington, DC 20036

[22] *Id.* at 24.

[23] *See, e.g.*, PrivacyRights Clearinghouse, *Chronology of Data Breaches*, http://www.privacyrights.org/sites/default/files/static/Chronology-of-Data-Breaches_-_Privacy-Rights-Clearinghouse.pdf.