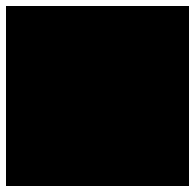


UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580



Office of the Secretary

October 13, 2011

Mr. Jeff Chester
Executive Director
Center for Digital Democracy
1220 L Street, NW
Suite 300
Washington, DC 20005

Re: *In the Matter of Google Inc., File No. 1023136, Docket No. C-4336*

Dear Mr. Chester:

Thank you for your comment on behalf of the Center for Digital Democracy (“CDD”) on the Federal Trade Commission’s consent agreement in the above-entitled proceeding. The Commission has placed your comment on the public record pursuant to rule 4.9(b)(6)(ii) of the Commission’s Rules of Practice, 16 C.F.R. § 4.9(b)(6)(ii), and has given it serious consideration.

consumer information and is committed to protecting consumer privacy. Toward that end, the order will require Google to build and maintain strong privacy protections for all its products and services going forward. Indeed, the order not only covers Google Buzz and Gmail; it applies broadly to all of Google’s products and services, including the ones mentioned in your comment.

The consent order mandates that Google establish and maintain a comprehensive privacy program that addresses privacy risks related to new and existing products and services and that protects the privacy and confidentiality of “covered information,”¹ among other provisions. While the proposed order sets forth several elements that the privacy program must include,

¹ “Covered Information” is defined in the order as “information respondent [Google] collects from or about an individual, including, but not limited to, an individual’s: (a) first and last name; (b) home or other physical address, including street name and city or town; (c) email address or other online contact information, such as a user identifier or screen name; (d) persistent identifier, such as IP address; (e) telephone number, including home telephone number and mobile telephone number; (f) list of contacts; (g) physical location; or any other information from or about an individual consumer that is combined with (a) through (g) above.”

some flexibility is afforded with regard to its implementation. This approach allows innovation in the area of privacy-enhancing technologies and is designed to keep pace with a dynamic marketplace. In particular, the privacy program must contain controls and procedures appropriate to Google's size and complexity that reflect the sensitivity of data handled, the scope and nature of Google's business activities, and the types of risks the company faces. To the extent that reasonably foreseeable, material risks arise from Google's products, services, and business practices, Google must use reasonable and appropriate procedures to address these risks or it cou