U.S. Consumer Product Safety Commission PRIVACY IMPACT ASSESSMENT				
Name of Project:	Recall Effectiveness Focus Groups			
Office/Directorate:	Division of Human Factors			
A. CONTACT INFORMATION				
Person completing PIA: (Name, title, organization and ext.)	Celestine Kiss, Engineering Psychologist			
System Owner: (Name, title, organization and ext.)	Celestine Kiss, Division of Human Factors, x7739			
System Manager: (Name, title, organization and ext.)	Amanda Kealey, the Polling Company, 202-667-6557			
B. APPROVING OFFICIALS	**Signature**	**Approve**	**Disapprove**	**Date**
System Owner				
Privacy Advocate	Linda Glatz, ITPP			
Chief Information Security Officer	Patrick Manley, ITTS	✓		4/3/07
Senior Agency Official for Privacy **System of Record** _____Yes _X_No	Mary Kelsey, Director, ITPP	✓		4/5/07
Reviewing Official:	Patrick D. Weddle, AED, EXIT	✓		4/5/07
C. SYSTEM APPLICATION/GENERAL INFORMATION				
1. Does this system contain any personal information about individuals? (If there is **NO** information collected, maintained, or used that is identifiable to the individual, the remainder of PIA does not have to be completed.)	Yes.			

D. DATA IN THE SYSTEM	
1. **What categories of individuals are covered in the system?** (public, employees, contractors)	General public.
2. **Generally describe what data/information will be collected in the system.**	The data in the system will consist of the potential participant's name, address, phone number and email address.
3. **Is the source of the information from the individual or is it taken from another source? If not directly from individual, then what other source?**	The information is obtained directly from the individual respondents.
4. **How will data be checked for completeness?**	Upon contact with the individual, data will be verified.
5. **Is the data current?** (What steps or procedures are taken to ensure the data is current and not out-of-date?)	Data is collected one time, and does not need to be updated unless the individual informs us of new information.
6. **Are the data elements described in detail and documented?** (If yes, what is the name and location of the document?)	Not applicable.
E. ATTRIBUTES OF THE DATA	
1. **Explain how the use of the data is both relevant and necessary to the purpose for which the system is being designed?**	The information in the data base will be used to contract potential participants in the focus groups. Name, address, phone number and email addresses are all necessary to contact and verify contact with the correct person.
2. **If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use? Explain.**	Not applicable.
3. **How will the data be retrieved? Can it be retrieved by a personal identifier? If yes, explain and list the identifiers that will be used to retrieve information on the individual.**	Information is retrieved by a structured search of the listed data. All searches and contacts are made at random, so each individual has an equal chance of being contacted. Personal identifiers can be retrieved only if a search is conducted in the body of personal communication or comment from the individual themselves, however, that is not the intended use of this database.
4. **What opportunities do individuals have to decline to provide information or to consent to particular uses of the information?**	Participation is strictly voluntary and therefore, they are free to decline at any time.
F. MAINTENANCE AND ADMINISTRATIVE CONTROLS	
1. **What are the retention periods of data in this system?**	The data will be retained for the length of the contract.
2. **What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?**	Upon completion of the contract, the original disk with be returned to the Project Officer at the Consumer Product Safety Commission. All contact information including names, email addresses, and telephone numbers provided by the Manufacturer will be removed from equipment including servers, computers, disc drives and other electronic equipment and storage media.
3. **Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.**	No.
4. **What controls will be used to prevent unauthorized monitoring?**	Not applicable.

5. Is this system currently identified as a CPSC system of records? If so, under which notice does the system operate?	No
6. If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain	Not applicable.
G. ACCESS TO DATA	
1. Who will have access to the data in the system? (e.g., contractors, managers, system administrators, developers, other).	The system manager will have access to the data in the system.
2. What controls are in place to prevent the misuse of data by those having access? (Please list processes and training materials.)	A restricted set of administrators are granted access to the data on a need-to-know basis. Controls to ensure data integrity and prevention of misuse include authorized login and password, firewall protection, as well as training procedures and management oversight of the entire work-flow process.
3. Who is responsible for assuring proper use of the data?	The system manager
4. Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?	Yes.
5. Do other systems share data or have access to the data in the system? If yes, explain. Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?	No.
6. Will other agencies share data or have access to the data in this system? If yes, how will the data be used by the other agency?	No.

To: Celestine Kiss, Engineering Psychologist, Division of Human Factors
U.S. Consumer Product Safety Commission

From: Kellyanne Conway, President & CEO
Amanda Kealey, Project Manager
the polling company™, inc. GSA Contract # GS-00F-0024P

Date: March 29, 2007

Re: Research Privacy Agreement

We are delighted that the **U.S. Consumer Product Safety Commission (CPSC)** is continuing to move forward with the "recall effectiveness" focus groups and are pleased to help with the process of gaining OMB approval. As instructed in the Modification 0003 to Contract CPSC-F-06-0088, this memo serves as documentation of the privacy provisions employed by **the polling company™, inc.** specifically in conducting qualitative research.

PRIVACY POLICY

the polling company™, inc./WomanTrend is committed to protecting the privacy of our clients, colleagues, and research participants. To prevent unauthorized access or disclosure, to maintain data accuracy, and to ensure the appropriate use of the information, **the polling company™, inc./WomanTrend** has in place appropriate physical and managerial procedures to safeguard the information we collect.

We do not collect information about the public or prospective participants unless they supply it knowingly and voluntarily. Focus group participation is completely voluntary and if individuals choose to partake, their identity and individual answers remain private. **the polling company™, inc./WomanTrend** uses personal information only to manage the scientifically designed collection of research data. As the data are collected, a respondent's individual data are considered confidential and is never shared with the public. In final reporting procedures, we only communicate aggregate data which do not identify individuals beyond a first-name basis.

In order to make contact with prospective participants, email addresses and associated personal information (such as name, phone numbers, and home addresses) are obtained from several sources. These sources include our clients (who provide us with lists of their customers), specialized list vendors, or individuals themselves. In each case, these persons are believed to have given permission to each of those entities to be contacted for research purposes.

We do not sell or share this information with any third parties other than as aggregate statistical data to fulfill the needs of our clients where appropriate and approved. We respect the integrity of the qualitative research process and do not attempt to sell or promote any product or service in the course of conducting research.

Employee access to contact information such as databases and client-provided sample lists is determined by their specific need to access such data in order to perform their assigned duties. Employees with access to the system include associates, analysts, managers, and directors, each of whom have executed confidentiality agreements in which they agree not to disclose such information to anyone outside of the company.

There are numerous internal controls in place to ensure data integrity and to prevent unauthorized access. These include firewall protection, LAN security and intrusion detection software, and a building security system that monitors visitors and requires keycards for after-hour access.

With respect to the software, all services are blocked, without exception, by firewall protection. Only authenticated and encrypted users are allowed remote access to the network. These steps ensure that neither sniffing (the practice of "listening in" on Internet communications) nor scanning (the act of probing a system for open programs) are permissible on the system. Other internal provisions include server protection that requires authentication for access allowing no unauthorized users access to internal files.

At the conclusion of the project, all names and identifiers are wiped from internal systems, including servers, computers, PCs, laptops, disc drives, and other electronic equipment and storage media. Materials provided at the start of each project by the client are returned to the client per their directive. Final deliverables such as written reports are sent directly to the client and are maintained in internal folders but are never shared with the public or other entities unless explicitly instructed to do so by the client.