Attachment C. GfK Privacy Procedures for Panelists and GfK and SSS Data Management Procedures

Privacy Protections for Panelists

Privacy Agreement with Panelists. The KnowledgePanel recruitment and empanelment process

is designed to comply with CAN-SPAM[1] and CASRO[2] guidelines. Further, our policies conform to

participant treatment protocols outlined by the federal Office Management and Budget, following

guidelines from the Belmont Report. Survey responses are kept secure to the extent permitted by law;

personally identifying information is never revealed to clients or other external parties without explicit

respondent approval and a client-signed nondisclosure agreement. When surveys are assigned to

KnowledgePanel panel members, they are notified in their password-protected email account that a

survey is available for completion. Surveys are self-administered and accessible any time of day for a

designated period. Participants can complete a password-protected survey only once. Members may

withdraw from the panel at any time, and continued provision of the web-enabled device (e.g., laptop or

netbook) and Internet service is not contingent on completion of any particular survey.

All KnowledgePanel panelists are given a link to access the GfK Privacy and Terms of Use Policy

electronically at all times via the Panel Member website and they also are able to review it at any time

on the Members Page and in links contained in survey invitations. In the privacy terms, there is a section

entitled the "Panel Member Bill of Rights" which summarizes the privacy protections for panelists and

explains that participants can decide whether to participate in the panel or to answer any survey

questions. It includes the following text:

   • We are researchers, not telemarketers. Here's what we can promise you:

---

[1] The CAN-SPAM Act is a law that sets the rules for commercial email.

[2] Council of American Survey Research Organizations

• We operate under the standards set by the Council of American Research Organizations (CASRO) [www.casro.org] and our Web site is approved by TRUSTe.

• Your survey responses and information are provided to our clients in an anonymous form, unless you have given your express permission.

• Occasionally, we may contact you to validate responses. We will never misrepresent ourselves, nor what we are doing.

• Your decision about participating in the KnowledgePanel or responding to specific questions will be respected without question.

Each KP member age 18 years of age or older can be categorized into one of four types:

1) A primary respondent living in a household with Internet access

2) A non-primary respondent living in a household with Internet access

3) A primary respondent living in household without Internet access

4) A non-primary respondent living in household without Internet access

The primary respondent is the individual with whom GfK initially directly communicated during the recruitment process, while the non-primary respondent is any other adult living in the same household as the primary respondent. For primary respondents, consent to receive survey invitations from KnowledgePanel is obtained during the recruitment process when primary respondents are asked to give their email addresses or shipping addresses to receive the web-enabled device in the following series of questions :

For each of your surveys, we send a personal invitation to your email address. The email message will have a link to the survey.

Our surveys are completed online. You can do them whenever you have free time and, if

necessary, pause in the middle and complete at a later time—although most surveys are brief. We will notify you when completing a survey that is time sensitive.

Being a panel member is easy and fun, and it allows you to earn cash by answering surveys. In fact, we will send you a one-time $10 check for completing your first survey called "Getting to Know You".

Your email address will be kept secure to the extent permitted by law. We can promise you that GfK will never share your email address with anyone without your permission.

Please enter your email address:

_____@_____

Please confirm that this is the email address you would like us to use to send your personalized survey invitations. [insert email address]

1. Yes, it is correct

2. No, I need to make a correction

They are then asked to complete the "Core Profile Survey" which collects basic personal demographic information. Primary respondents must complete the "Core Profile Survey" to become empaneled and before receiving invitations to answer client surveys.

Consent from non-primary respondents is obtained during the initial online survey when respondents answer "Yes" to the question:

Now that you know a little more about the KnowledgePanel, would you like to join and have your opinion heard?

1 Yes

2 No

Similar to primary respondents, non-primary respondents must then complete the "Core Profile Survey" before answering any client surveys.

Data Management Procedures

GfK Data Management Procedures. All survey responses will be maintained in a secure manner, with identifying information never revealed without respondent approval. GfK uses advanced security measures to protect against the loss, misuse, and alteration of information provided to GfK. To enhance data security, the GfK Web server supports SSL (Secure Socket Layer) Encryption security technology and access to the GfK database is restricted to portals that only GfK controls. In addition, all panel members are required to use passwords and usernames.

GfK warrants that all employees are bound to protect the privacy of all personal information provided by respondents, and very few employees actually have access to any sensitive, personally identifiable data. The only staff members who have access to this information—personally identifying information about panel members—are those with a direct need to know. Therefore, the only persons with access are the following:

> • Database and IT administrators with access to computer servers for the purpose of maintaining the computers systems at GfK;

> • Staff members in the Panel Relations department that have direct contact with panel members as part of the inbound and outbound call center operations. These staff members are responsible for troubleshooting any problems panelists might be having with their equipment or

software related to survey administration, incentive fulfillment, and panel management.

• Staff members of the Statistics department have access to personally identifying information in order to draw samples for the various surveys we conduct at GfK.

At GfK, all personally identifiable information (PII) such as names, addresses, emails, etc. are kept secure to the extent permitted by law in a separate office in the Information Technology section of the main offices in Palo Alto, CA. All data transfers from web-enabled devices (PCs and laptops used for survey administration) to the main servers pass through a firewall. GfK never provides any respondent's personal identifiers to any external client or agency without the respondent's explicit and informed consent. The client or agency must also sign a nondisclosure agreement. PII is never provided to anyone outside of GfK in combination with the survey response data unless explicitly permitted in a consent form and nondisclosure agreement.

All electronic survey-specific data records are stored in a separate secured database that does not contain PII. Staff members who have access to the PII, which is limited to the Panel Management staff members, do not have access to the survey response data, and vice versa, with the exception of IT administrators who must have access to maintain the computer systems. The secured database contains field-specific permissions that restrict access to the data by type of user, as described above, thus preventing unauthorized access.

The survey response data are identified only by an incremented ID number. The personally identifying information is stored in a separate database that is accessible only to persons with a need to know, as described above. The survey data extraction system exports only anonymized survey data identified only by the Panel Member ID number. The data analysts with access to the survey data extraction system, as

they do not have access to personally identifying information, cannot join survey data to personally

identifying data. Panel Relations and Statistics staff members do not have access to the survey data

extraction system, and therefore cannot join survey data to personally identifying data.

A system of standard operating procedures have been put in place for documenting all processes

relating to keeping the identities of panel members secure to the extent permitted by law. GfK retains

the survey response data in its secure database after the completion of a project. These data are

retained for purposes of operational research, such as studies of response rates and for the security of

our customers who might request at a later time additional analyses, statistical adjustments, or

statistical surveys that would require re-surveying research subjects as part of validation or longitudinal

surveys.

SSS Procedures for Data Handling and Management

Using secure procedures, GfK will send electronically to SSS a dataset of all survey data, including all

documentation, weights, and complete variable and value labels. This will be done approximately one

week after the closing of GfK's NNDS data collection operations. The data will be handled in a protected

and secure manner while ensuring data integrity, using SSS processes and procedures for all

aspects of handling data. Only authorized NDEP project team users will be allowed access to

the data. SSS has a thorough Security Plan that addresses all aspects of data security, including data

access, management, proper storage, and disposal. SSS also has encryption software in place, where

required. All SSS business-critical systems have backups and redundancy on site in case of server failure.

SSS also can store data and software backup files offsite at its secure data center in Ashburn, VA.