LCC and Blunt Use Audience Insights Survey – Privacy Information

Here are our privacy protections and rationale for collecting each type of PII:

RTI stores PII separately from IP address, which is stored separately from survey responses. All PII (e-mail address, Facebook unique ID, birthdate, zip code) will be collected within the Qualtrics survey platform, downloaded by RTI, and stored by Qualtrics as one file that contains only PII including a RTI-assigned unique study ID. We are using the study ID to connect screener data and survey data and to determine if a participant has completed the survey. Study IDs will not be shared with the participants or FDA but will be included in the survey data on the project share and the PII data on the FIPS Moderate Network. The Facebook unique ID is assigned by Facebook to identify each account. Some Facebook users do not have an email address, but every Facebook user has a Facebook unique ID associated with their account. The Facebook unique ID will allow us to identify potential duplicate respondents. Collecting the Facebook unique ID does not add risk as both the Facebook unique ID and Facebook email (if included) can be used to locate a Facebook account.

IP address will be collected by Qualtrics, downloaded by RTI, and stored by Qualtrics and RTI as a separate second file that only contains IP address, the study ID, and the participant responses to the screener.

Responses to the survey questions will be collected by Qualtrics, downloaded by RTI, and stored by RTI and Qualtrics as a separate third file. IP address and e-mail address will not be collected in the same file.

All of the data files (PII, screener data (with IP address), and survey data (study ID but no other PII or IP address))) will be downloaded as separate files from Qualtrics (which requires a password). The password to access the survey data files will not be shared with FDA. Since the FIPS Moderate Network does not permit access to the internet (and downloading the data from Qualtrics requires an internet connection), the data files will be downloaded from Qualtrics to a secure RTI study share drive. The files will be stored on the study share drive for 48 hours after download while fraud detection procedures are completed. Fraud detection measures involve combining IP address, e-mail address, and screener responses. Study staff, who have documented training in human subjects protection, are granted as-needed access to the data on the share drive. Once fraud detection procedures have been completed (within 48 hours after download), all files containing PII will be moved to the FIPS Mod Network where it will be stored for 3 years after the project has ended. If the FIPS Mod Network is unavailable because of an RTI outage, we will move files with PII to the FIPS Mod Network as soon as access is restored. As an additional quality control, a second study team member will confirm that PII has been moved to the FIPS Mod Network after fraud protection procedures have been completed. The file containing study ID and the survey responses will remain on the

study share drive. At the completion of data collection, the databases will be deleted from our Qualtrics account and remain only on RTI's secure shared drive and FIPS Mod Network.

E-mail address is necessary for all participants, even those who screen out as ineligible, for fraud detection purposes (we have to be able to detect and eliminate duplicates across both eligible and ineligible screener completes). As a result, it is not possible to route participants to the screener exit if they screen out as ineligible before collecting their e-mail address. E-mail addresses will be shared with Creative Group for incentive purposes only. No respondent identifiers will be contained in reports to FDA and results will only be presented in aggregate form.

We will advise respondents to situate themselves so that others cannot see their answers as they complete the survey. The online survey is programmed so that only one sensitive question appears on each screen, and so it is not possible to go back through the survey. These procedures make it easier for participants to hide responses from others who may be in the vicinity when they are completing the survey. The survey is also programmed to log respondents out after an hour of inactivity. Respondents may choose to respond "prefer not to answer" to any question and may drop out of the survey at any time for any reason.

The data's integrity and availability are protected by security controls selected and implemented in the course of providing the data collectors with an authority to operate (ATO). Controls are selected based on National Institute of Standards and Technology's (NIST) guidance concerning the ATO process, appropriate to the system's level of risk as determined using NIST's Federal Information Processing Standards (FIPS) 199. RTI performs annual reviews to evaluate user access. Data discrepancies identified in the course of data collection are addressed when discovered.

Security for respondents completing the online surveys will be assured in a number of ways: (1) we will screen out youth under the age of 15, (2) Participants will log onto the secure server hosted by Qualtrics using a link provided in the completed screener and the unique identifier, (3) respondents will be provided with information about the privacy of their data before they encounter the first survey item, (4) respondents will be required to provide their assent or consent to freely participate before they encounter the first survey item, and (5) respondents will have the option to decline to respond to any item in the survey for any reason. All who handle or analyze data will be required to adhere to the standard data security policies of RTI.

PII will not be included in any internal or external report. Data will not be reported in such a way that it will be possible to identify any individual participant.