Federal Trade Commission
Privacy Impact Assessment

Web Customer Satisfaction Surveys (ForeSee)

Updated June 2019

Table of Contents

1 System Overview

1.1 Describe the project/system and its purpose.

The Federal Trade Commission uses ForeSee online surveys (acquired by Verint) to get feedback from users of the agency's websites. The FTC uses the responses to the surveys to measure website visitors' overall satisfaction with the sites. The FTC also uses ForeSee to gain insights about the types of information visitors were looking for, whether they were able to find that information, and challenges they might have encountered during their visit. A randomly selected segment of visitors to ftc.gov, ftccomplaintassistant.gov, consumer.ftc.gov, consumidor.ftc.gov, and bulkorder.ftc.gov receive an invitation to complete the survey. The FTC uses the customer satisfaction scores provided by the system to report as part of the agency's quarterly reporting for the Government Performance and Results Act (GPRA).

ForeSee collects three general categories of information: information provided by the survey recipients, information provided by FTC ForeSee administrators, and information collected automatically by the application.

From Survey Recipients:

The survey collects answers to a series of questions from website visitors who choose to respond to the survey.

The survey includes model questions that everyone sees. These have to do with the design of the site, the performance of the site, the site navigation, and the thoroughness of the information.

The survey also includes custom questions that may ask respondents about the information they were looking for and whether they were able to find it, if they did a search on the site, and if they have suggestions about how to improve the site, their role (i.e., consumer, businessperson, lawyer, etc.) and their age group.

From FTC ForeSee Administrators

ForeSee collects usernames and passwords from backend FTC users of the ForeSee application.

From Application:

The application collects site usage data, such as:

- how many pages each visitor to the website has viewed
- what page the visitor was viewing when the survey appeared
- what language, browser and operating system the visitor is using
- the referring website
- search terms that brought the visitor to the website

This data does not link back to individuals. The site usage data above is linked to the SurveyID (also known as Respondent ID). This ID number is randomly generated when the survey is presented to the respondent and is not linked to any other personally identifiable information.

1.2 What specific legal authority allows for the collection, maintenance, or dissemination of information for this project/system?

The FTC Act authorizes the FTC to prevent unfair and deceptive acts and practices in interstate commerce and, in furtherance of this mission, to gather, compile, and make information available in the public interest. See 15 U.S.C. 45, 46(a), (f).

In addition, the Office of Management & Budget (OMB) Memorandum (June 13, 2011) on implementing Executive Order 13571, Streamlining Service Delivery and Improving Customer Service, calls on agencies to solicit timely feedback in order to improve the quality of services.

The U.S. Department of the Interior's Federal Consulting Group, which procures ForeSee Results services and technology on behalf of federal agencies, has obtained clearances from the Office of Management and Budget for customer satisfaction surveys under the Paperwork Reduction Act.

2 Data Type, Sources, and Use

2.1 Specify in the table below what types of personally identifiable information (PII)[1] may be collected or maintained in the system/project. Check all that apply.

PII Elements: This is not intended to be an exhaustive list. Specify other categories of PII as needed.		
☐ Full Name	☐ Biometric Identifiers (e.g., fingerprint, voiceprint)	☒ User ID
☐ Date of Birth	☐ Audio Recordings	☐ Internet Cookie Containing PII
☐ Home Address	☐ Photographic Identifiers (e.g., image, x-ray, video)	☐ Employment Status, History, or Information
☐ Phone Number(s)	☐ Certificates (e.g., birth, death, marriage, etc.)	☐ Employee Identification Number (EIN)
☐ Place of Birth	☐ Legal Documents, Records, Notes (e.g., divorce decree, criminal records, etc.)	☐ Salary
☐ Age	☐ Vehicle Identifiers (e.g., license plates)	☐ Military Status/Records/ ID Number
☐ Race/ethnicity	☐ Financial Information (e.g., account number, PINs, passwords, credit report, etc.)	☐ IP/MAC Address
☐ Alias	☐ Geolocation Information	☐ Investigation Report or Database
☐ Sex	☐ Passport Number	☐ Driver's License/State ID Number (or foreign country equivalent)
☐ Email Address		☒ Other *(Please Specify)*: Open text fields in survey, passwords of FTC backend users.
☐ Work Address		
☐ Taxpayer ID		
☐ Credit Card Number		
☐ Facsimile Number		
☐ Medical Information		
☐ Education Records		
☐ Social Security Number		
☐ Mother's Maiden Name		

The survey is not intended to collect PII from members of the public. However, users are not prevented from entering it into the open text fields of the survey. The FTC is exercising its discretion to conduct a PIA to document possible risks to PII that may be unintentionally collected by the agency via these open text fields, and to document the application's use of cookies.

2.2 What types of information other than PII will be collected, disseminated, or maintained by the project/system? Provide a general description below and be sure to include all data elements.

As noted in Section 1.1 above, the application collects the content of survey responses from users, and it also collects site usage data automatically.

2.3 What is the purpose for collection of the information listed above?

From Survey Recipients:

[1] Per OMB Circular A-130, personally identifiable information (PII) means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

The FTC collects user feedback to measure the effectiveness of our websites and to plan improvements to the sites.

From FTC ForeSee Administrators:

Usernames and passwords are collected for secure login purposes.

From application:

The survey collects site usage data to ensure that a visitor has browsed enough pages on the site to be able to answer the questions in the survey.

2.4 What are the sources of the information in the system/project? How is the information collected?

Source of Data	*Type of Data Provided & How It Is Collected*
Survey Recipients	The survey respondents who choose to complete the survey provide answers based on their experience with the website. Some questions provide a series of answers respondents can select. Other questions are open-ended and allow respondents to type their replies.
FTC ForeSee Administrators	FTC ForeSee Administrators enter their own usernames and passwords into the application.
Application	Each survey respondent is assigned an identifier called the SurveyID: a system identifier generated by the code to represent the survey presented to the visitor. See 1.1 for more information about SurveyID. The system uses session and persistent cookies: for further information, see Section 7.1 and 8.1.

3 Data Access and Sharing

3.1 In the table below, specify the systems/applications and groups (both FTC and non-FTC) that will have access to or share data in the system/project.

Data Will Be Accessed By and/or Provided To:	*How and Why the Data Will Be Accessed/Shared*
FTC staff/contractors	Website managers will have access to the information through an online portal and may share this information with others in the agency in anonymous forms.
Contractors employed by Verint (the ForeSee vendor)	Client Services staff at Verint with a reason to access government clients will have access to the information.

3.2 Do contractors and/or third party service providers have access to data in the project/system? If yes, explain what privacy requirements are in place to ensure that data is properly protected.

Yes.

The risk of harm due to contractor misuse of PII in this application is low. As noted above, the survey is not intended to collect PII from members of the public, although users are not prevented from entering it into the open text fields of the survey.

Nevertheless, the vendor has controls in place to protect the data in the application. See section 5.2 for more information.

☐ Not Applicable.

3.3 If you answered "yes" to 3.2, describe the privacy incident response plan maintained by the contractor's organization or third party service provider.

☐ Not Applicable.

4 Notice and Consent

4.1 How are individuals provided with notice prior to the collection of their PII? If notice is not provided, explain why.

☐ Notice is provided via (*check all that apply*):
- ☐ Privacy Act Statement (☐ Written ☐ Oral)
- ☐ FTC Website Privacy Policy
- ☐ Privacy Notice (e.g., on Social Media platforms)
- ☐ Login banner

☒ Other (*explain*): A percentage of visitors will receive invitations to take the survey. Those who choose to take the survey will see the survey questions. The survey includes an explanation of how and why the information will be collected and used. The survey invitation and the survey itself will link to the Privacy Policy.

☐ Notice is not provided (explain): _____

4.2 Do individuals have the opportunity to decline to provide information or to consent to particular uses of their information (other than required or authorized uses)?

Yes. Visitors can choose not to complete the survey. Respondents who have begun the survey can abandon the survey at any time. If that happens, any information entered into the form will be discarded. This does not necessarily discard information collected automatically by the application, however.

If a person completes the survey, they agree to have their answers included in the survey data. They cannot choose particular uses of the information. However, the information will be used as described in this PIA.

4.3 Are there procedures in place to allow individuals access to their personally identifiable information? Explain.

Because the system collects the survey data through an anonymous process, users will not be able to gain access to their information after they complete the survey.

4.4 Are there procedures in place to allow individuals the ability to correct inaccurate or erroneous information? What is the process for receiving and responding to complaints, concerns, or questions from individuals? Explain.

Not applicable. See 4.3 above.

5 Data Accuracy and Security

5.1 Are there procedures in place to ensure that the information maintained is accurate, complete, and up-to-date?

The FTC cannot check the answers submitted by respondents for timeliness or accuracy: respondents voluntarily provide answers based on their experience with the site, and the FTC assumes those responses are accurate.

5.2 Are there administrative procedures and technical safeguards in place to protect the data in the system/project? What controls are in place to ensure proper use of the data? Please specify.

Yes.

Some administrative procedures and technical safeguards apply specifically to ForeSee:

As noted on ForeSee's online security documentation, "ForeSee provides end-to-end 128-bit encryption of all hosted resources using TLS 1.2 protocol." See the online security documentation for more information.

The applicable contract between the Federal Consulting Group and the FTC provides that collecting, analyzing, and reporting of the data will be conducted in full compliance with the Privacy Act of 1974. The Federal Consulting Group is also responsible for ensuring compliance with all other applicable IT security requirements and procedures.

In addition, the contractor, Verint, recognizes that the European Union has established strict protections regarding the handling of EU Personal Data, and ForeSee Results therefore has elected to adhere to the US-EU Safe Harbor Privacy Principles with respect to such EU Personal Data and Personal Data that it receives in the United States.

Verint Client Services staff completes privacy training annually during company-wide security training. There are additional trainings on a semiannual basis for Satisfaction Research Analysts (SRA) on how to handle client data. This is defined in Verint's procedures and policies documentation.

Each FTC application administrator will have a unique login and password and will not share login credentials with anyone else. FTC application administrators will use strong passwords and will change them on a regular basis in accordance with FTC policy.

The application also validates survey submissions to make sure that they come from approved URLs and survey code.

Other administrative procedures and technical safeguards apply not only to ForeSee, but to many other applications at the FTC, as well:

All FTC positions are assigned a risk designation that has associated criteria for personnel screening. All potential FTC employees, contractors, and volunteers are subject to background investigations and suitability reviews in accordance with OPM guidance. Before any new employee, contractor, or volunteer can access FTC applications, that individual must first attend new employee orientation and successfully complete the FTC's Privacy and Security Awareness training. All employees are granted basic network access to include email services, the Internet, the Intranet, network shared drives, network-based applications, and are assigned their own home directory. Categories of employees deemed to be higher risk – such as interns and International Fellows – may have restricted access to network and physical space.

Supervisors and/or Contracting Officer's Representatives (CORs) must identify and approve employee requests to access network applications and specify the appropriate user role and level of access privileges. Auditing measures and technical safeguards are in place commensurate with the Moderate-Impact Baseline of the National Institute of Standards and Technology (NIST) Security and Privacy Controls for Federal Information Systems and Organizations Special Publication (SP) 800-53.

FTC staff is responsible for minimizing PII and disposing of it when the PII is no longer needed and in accordance with appropriate records disposition schedules. The FTC ensures that all staff and contractors annually electronically certify their acceptance of FTC privacy responsibilities and procedures by requiring comprehensive Information Security and Privacy Awareness training. Moreover, all staff must annually acknowledge procedures for handling PII – including minimizing PII – and attest that all PII maintained by the individual has been properly secured and accounted for as part of the FTC's annual privacy and security training.

5.3 Is PII used in the course of system testing, training, or research? If so, what steps are taken to minimize and protect PII during this process?

.

☒ Not Applicable

6 Data Retention and Disposal

6.1 Specify the period of time that data is retained in the system/project. What are the specific procedures for disposing of the data at the end of the retention period?

The data will be retained and disposed of in accordance with applicable schedules issued or approved by the National Archives and Records Administration (NARA). More broadly, all data will be deleted/destroyed in accordance with Office of Management and Budget, NARA, and National Institute of Standards and Technology regulations and guidelines. In the instance in which a responded chooses to provide sensitive personal information, despite instructions to the contrary, FTC staff will work with ForeSee to immediately delete such data. This unique issue aside, data will be available through the online portal for as long as ForeSee Results continues to provide services to the FTC, because the FTC plans to compare customer satisfaction over time and to keep records of these changes.

Because the survey is not intended to collect personally identifiable information, there are no significant privacy risks associated with the disposal of survey data.

7 Website Privacy Evaluation

7.1 Does the project/system employ the use of a website? If so, describe any tracking technology used by the website and whether the technology is persistent or temporary (e.g., session cookie, persistent cookie, web beacon). Describe the purpose of using such tracking technology.

This application, which runs on various ftc.gov websites, uses single-session cookies and persistent cookies.

The use of single-session cookies only applies to visitors who choose to complete the survey and the impact it has is minimal, if any exists at all. The survey uses single-session cookies to track site usage information as described in 1.1. Single-session cookies do not collect personally identifiable information or IP addresses. The system automatically deletes the single session cookie when the visitor closes the browser. The single session cookie presents a low privacy risk because it does not collect any personally identifiable information and will not be used to track visitors once they leave the site.

The survey uses a persistent cookie to track if a respondent was presented the survey and if the person completed or declined the survey. This helps ensure that a respondent who declined doesn't receive the survey again with 30 days. The persistent cookies in the survey do not collect personally identifiable information

☐ Not Applicable

8 Privacy Risks and Evaluation

8.1 Considering the type of information collected and sources of collection, what privacy risks were identified and how were these risks mitigated?

Risk	***Mitigation Strategy***
Unnecessary collection of personally identifiable information, including sensitive personal information	It is possible that survey respondents could include personally identifiable information in their open-ended responses to a few questions. If we discover that a survey respondent has included sensitive personal information, we will work with the contractor to delete that information from the system. Generally, FTC websites are not intended for children under 13, and the survey is not intended to collect any personally identifiable information from children under 13. If the FTC or the contractor discovers that we have inadvertently gathered

	any such information for a child under 13, the FTC will work with the contractor to delete it immediately. See also section 1.1 above.
Inappropriate tracking of users via cookies	See Section 7.1 above. See also Section 1.1 above.
Unauthorized access to the application	FTC staff will have access to the system only as needed. Only individuals tasked with retrieving or analyzing the data to measure the effectiveness of the FTC websites and to plan improvements to the sites will have access to the survey data. Program managers may share information from the system but only in anonymous or aggregate forms. At Verint, access to survey data is limited to the Client Services staff with a reason to access government clients. See also Section 5.2.

8.2 Does the project/system employ the use of automated privacy controls or enhanced capabilities designed to support privacy? Explain.

See sections 5.2 and 8.1.

8.3 Has a Privacy Act System of Records Notice (SORN) been published in the Federal Register for this system/project? If so, list the applicable SORN(s).

Not applicable: records within this application are not retrieved using a person's name or other unique identifier.

8.4 How does the project/system ensure that the information is collected, used, stored, or disseminated in accordance with stated practices in this PIA?

The Privacy Office routinely collaborates with system/application owners as part of its Privacy Continuous Monitoring Strategy to ensure that the information in PIAs, including this one, is accurate and to mitigate any privacy risks, as needed. Members of the public with questions or comments on the FTC's privacy practices may contact the Chief Privacy Officer using the contact information at ftc.gov/privacy.

9 Appendix: Privacy Controls Cross-Walk

Question	Applicable Control(s)
1.1, 2.3	AP-2, Purpose Specification
1.2	AP-1, Authority to Collect
2.1	SE-1, Inventory of Personally Identifiable Information
2.3	DM-1, Minimization of PII
3.1	UL-1, Internal Use UL-2, Information Sharing with Third Parties
3.2	AR-3, Privacy Requirements for Contractors and Service Providers AR-5, Privacy Awareness and Training
3.3	SE-2, Privacy Incident Response
4.1	TR-1, Privacy Notice TR-3, Dissemination of Privacy Program Information
4.2	IP-1, Consent
4.3	IP-2, Individual Access
4.4	IP-3, Redress IP-4, Complaint Management
5.1	DI-1, Data Quality DI-2, Data Integrity and Data Integrity Board
5.3	DM-3, Minimization of PII Used in Testing, Training, and Research
6.1	DM-2, Data Retention and Disposal
8.1	AR-2, Privacy Impact and Assessment
8.2	AR-7, Enhanced System Design and Development
8.3	TR-2, System of Records Notices and Privacy Act Statements AR-8 Accounting of Disclosures
8.4	AR-4, Privacy Monitoring and Auditing