UNITED STATES DEPARTMENT OF AGRICULTURE

ARS Azure Applications

Privacy Impact Assessment

Document Revision History

Row #	Document & Version, Release or Build Number	Revision Date	Revision Author	Revision Description	Revision Tracking Noted
1	V1.0	2/15/2022		Final	Git hub issue Tracker #211
2	V1.1	12/09/2022	Ursula Pieper	ATO Tasks Oct 2022 Updated filename / version # / Revision History Table	Annual update
3	V1.2	09/12/2023	Ursula Pieper	Add Privacy Officer's Signature	Azure Yearly Assessment

Policy, E-Government and Fair Information Practices

Privacy Impact Assessment for the

Agricultural Research Services (ARS) Azure Applications
Dec 10, 2021

Contact Point

Ursula Pieper
Associate Director
ITSD NAL Team Lead
Research, Education, and Economics Mission Area
Agricultural Research Services, Administrative and Financial Management
National Agricultural Library, Information Systems Division
202 734 8837
Ursula.Pieper@usda.gov

Reviewing Official

Lorna J. Drennen
Assistant Chief Information Officer
Agricultural Research Services
United States Department of Agriculture
(202) 720-3012
lorna.drennen@usda.gov

Abstract

The name of the system is ARS Azure Applications, with the child systems ARS Azure Infrastructure, ARIS Applications, ARS Public Websites, NAL Azure Applications, and GRIN Azure Applications.

The purpose of the system is to (i) provision the ARS Agricultural Research Information System (ARIS) to USDA staff and collaborators, and (ii) provide access to ARS, REE, inter-departmental, and collaborative web-based applications to USDA researchers, the international agricultural community, and/or the general public.

A PIA is being conducted after determination through the PTA. The ARIS Applications child system is storing sensitive PII (SSNs).

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

Introduce ARSAZURE and child systems, note that only ARIS contains sensitive PII, the system is owned by ARS, ARIS is owned by ARS HQ.

Describe full system/program, get this also from SSP. Performance and Awards sub-system contains PII.

- The system name and the name of the Department component(s) who own(s) the system;
- The purpose of the program, system, or technology and how it relates to the component's and Department's mission;
- A general description of the information in the system;
- A description of a typical transaction conducted on the system;
- Any information sharing conducted by the program or system;
- A general description of the modules and subsystems, where relevant, and their functions; and
- A citation to the legal authority to operate the program or system.

The ARS Azure Applications system (ARSAZURE), comprises the child systems ARS Azure Infrastructure, ARIS Applications, ARS Public Websites, NAL Azure Applications, and GRIN Azure Applications. The purpose of the system is to (i) provision the ARS Agricultural Research Information System (ARIS) to USDA staff and collaborators, and (ii) provide access to ARS, REE, inter-departmental, and collaborative web-based applications to USDA researchers, the international agricultural community, and/or the general public.

All child systems are owned by the USDA REE Agricultural Research Services (ARS), with ARS Headquarter owning the child systems ARIS Applications and the ARS public websites, the ARS National Agricultural Library (ARS-NAL) owning the NAL Azure applications, and the ARS Germplasm Resources Information Network owning the GRIN Azure Applications.
The ARSAZURE Authorization to Operate (pending) is the legal authority to operate the system.

Purpose of the Systems

ARS Azure Infrastructure

The infrastructure in Azure is a child system that is shared by all three Application child systems, and includes the connection to ARSNet through the USDA ExpressRoute for internal access to the Hub and shared services vnet (HSS) for developers, systems administrators, the web-application gateway, Cisco firewalls. The ARS Azure Infrastructure system components are shared between the ARIS Applications, the ARS Public Websites, the NAL Azure Applications, and the GRIN Azure Applications.

ARS Cyber

The ARS Cyber Child System provides an area within ARS Azure with full network access to the other child systems for the ARS Cyber team and ISC. It comprises security scanners and jump boxes.

ARIS Applications
The ARIS Applications provide essential mission applications supporting ARS and REE agencies research and administrative functions, including research program management, financial management, agreements, human resources, information technology, acquisition, and travel. Authentication is provided by USDA eAuthentication/LincPass access to privileged users only and data access is limited to need-to-know basis controlled by database accounts and roles. Major system components include Microsoft Windows servers running Oracle Weblogic, Oracle Database and Oracle Forms/Reports software. The ARIS Applications system is the only system that contains sensitive PII.

- A typical transaction involves entering and tracking research project and resource management data that is linked to REE personnel data downloaded from the National Finance Center (NFC). For example, telework program data for each REE employee is entered, reviewed, tracked and reported on to effectively manage the REE telework program.

ARS Public Websites

The ARS public websites display Agency-wide content covering information on ARS National Programs, to news and events, to career information as well as AgMagazine's Tellus and the Scientific Discoveries site. The site also supports ARS Area and research unit's web-sites. ARS web-sites host publicly available content that does not require authentication. Major system components include Microsoft Windows and Linux servers. Drupal and Umbraco are used for web content management.

NAL Azure Applications

The NAL Azure Applications include public websites from the ARS National Agricultural Library (NAL). Major system components include Linux servers and Microsoft Windows servers. These host publicly available content that do not require authentication and USDA only content. Web sites are managed through NGINX and Apache webservers and include a variety of open source and in-house developed software including Drupal, Java, JavaScript frameworks, Omeka, and other technologies.

Germplasm Resources Information Network (GRIN) Azure Applications

The Germplasm Resources Information Network (GRIN) documents USDA animal, microbial, and plant collections through informational pages, searchable databases, and links to USDA-ARS projects that curate the collections. GRIN is operated by the National Germplasm Resources Laboratory in Beltsville, MD. The National Genetic Resources Advisory Council represents U.S. agricultural stakeholders and provides recommendations to the Secretary of USDA on national policies related to agricultural genetic resources. The GRIN Azure Applications provide a laboratory notebook functionality to ARS GRIN researchers and make the information available to the general public. The GRIN applications are deployed on Microsoft Windows servers and use .NET and SQL Server database technologies.

Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed.

1.1 What information is collected, used, disseminated, or maintained in the system?

Add a section for each Child System

- **ARS Azure Infrastructure**

  - The information collected in this child system is only of technical nature, as this child system comprises the firewall, web application gateway, and other infrastructure components.
- **ARS Cyber**
  - The information collected in this child system is only of technical nature, as this child system comprises security scanners and jump boxes.

- **ARIS Applications**
  - The ARIS Applications child system is an integral ARS application for internal agency use that includes information about HR records.   This application contains information about research projects, employee names, employee social security numbers, employee positions, employee performance management information, employee assignments, grades, retirement dates, employee dates of birth, employee identification numbers (EMPID), passport numbers, and salary allocations.
- **ARS Public Websites**
  - The ARS Public Websites child systems provides information on ARS research to the general public. The information on ARS staff, office address, phone numbers, and email addresses.
- **NAL Azure Applications**
  - The NAL Azure Applications provide general agricultural information and ARS research results to the general public. These include content from the information centers at NAL: AgLaw documents, Animal Welfare Act documents and history, Food and Nutrition information and the Food Data Central Application, content from the Food Safety Information Office, digital exhibits from the library collection, catalogs of the library collection, Library specific document delivery, scientific data applications, informational websites from the National Invasive Species Information Center, content from the Federal Interagency Committee on Invasive Terrestrial Animals and Pathogens, the main website for the REE mission area, and the website of the Naree Advisory Board of REE.
- **GRIN Azure Applications**
  - The Germplasm Resources Information Network (GRIN) documents USDA animal, microbial, and plant collections through informational pages, searchable databases, and links to USDA-ARS projects that curate the collections. GRIN is operated by the National Germplasm Resources Laboratory in Beltsville, MD. The National Genetic Resources Advisory Council represents U.S. agricultural stakeholders and provides recommendations to the Secretary of USDA on national policies related to agricultural genetic resources. The GRIN Azure Applications provide a

laboratory notebook functionality to ARS GRIN researchers and university collaborators, and to make the information available to the general public.

1.2 What are the sources of the information in the system?

- **ARS Azure Infrastructure**
  No information source apart from general technical configurations
- **ARS Cyber**
  No information source apart from general technical configurations
- **ARIS Applications**

Information is acquired directly from employees from various functional areas (research, acquisitions, budgeting, etc.). PII related to personnel data is imported from the USDA National Finance Center (NFC) (e.g., name, date of birth, position, etc.).

- **ARS Public Websites**
  ARS research project data is collected from ARIS, ARS personnel data (name, office address, phone numbers, email addresses) is collected from the REE Directory and site data is provided by local web content managers.
- **NAL Azure Applications**
  The NAL general and special collections; Literature information collected by NAL curators; Staffing information from the agency; ARS research results.
- **GRIN Azure Applications**
  ARS GRIN Researchers
  University Collaborators

1.3 Why is the information being collected, used, disseminated, or maintained?

- **ARS Azure Infrastructure**
  No information is maintained apart from general technical configurations
- **ARS Cyber**
  No information is maintained apart from general technical configurations
- **ARIS Applications**
  The information is collected and disseminated to support the Agency's mission (Agricultural Research) and facilitate unique identification of personnel for human resource transactions.
- **ARS Public Websites**
  The information is being collected and disseminated to fulfill the mission of ARS and to fulfill the federal government's open data mandate.
- **NAL Azure Applications**
  The information is being collected and disseminated to fulfill the mission of the

National Agricultural Library and to fulfill the federal government's open data mandate.

- **GRIN Azure Applications**
  The information is collected to provide laboratory notebook functionality to ARS GRIN researchers, and to disseminated to fulfill the federal government's open data mandate.

1.4 How is the information collected?

- **ARS Azure Infrastructure and ARS Cyber**
  N/A
- **ARIS Applications**
  The information is collected by a combination of manual entry by functional users, manual imports from other sites, and imported from the USDA NFC.
- **ARS Public Websites**
  The information is collected by a combination of manual entry by local web content managers and imported from ARIS and the REE Directory.
- **NAL Azure Applications**
  The information is collected by a combination of manual curation by library staff, automated and manual literature mining, data and publication upload from USDA researchers to fulfill the open data mandate, automated upload from ARS research groups.
- **GRIN Azure Applications**
  The information is collected through direct upload from GRIN researchers, who use the system as a laboratory notebook.

1.5 How will the information be checked for accuracy?

- **ARS Azure Infrastructure and ARS Cyber**
  N/A
- **ARIS Applications**
  Information is verified during input and checked against other records. Approval processes associated with data processing along with checks and balances built into the system ensure accurate data entry and data integrity.
- **ARS Public Websites**
  Information is verified for accuracy by the local web content managers, by agency communications staff and by the web administrator.

- **NAL Azure Applications**
  The information is checked for accuracy by either the researchers that upload the data, or through manual curation by library staff and subject matter experts.
- **GRIN Azure Applications**
  The information is checked for accuracy by the technicians, curators, and researchers that make the data available.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

- ARS Azure Infrastructure (i)
- ARS Cyber (i)
- ARIS Applications (i, ii)
- ARS Public Websites (i)
- NAL Azure Applications (i)
- GRIN Azure Applications (i)

  - The OPEN Government Data Act (included as Title II in Speaker Ryan's Foundations for Evidence-Based Policymaking Act (FEBP) H.R. 4174) (i)
  - The paperwork Reduction Act of 1995 (i)
  - FISMA (i)
  - Privacy Act of 1974 (5 U.S.C. $552a, Note) (ii)
  - Social Security Act Section 205(c)(2)(c)(viii) (ii)

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

- **ARS Azure Infrastructure and ARS Cyber**
  Minimal privacy risks
- **ARIS Applications**
  Given the type of data collected, processed, and stored within the system, the agency recognizes the risk of inadvertent privacy data disclosure. The risk is mitigated through a series of security measures built into the infrastructure and the system. Detailed description of implemented system security controls can be found in the system security plan. Application security controls are provided by USDA eAuthentication/LincPass access limited to authorized users only and data access is limited to "need to know" basis controlled by database accounts and roles.
- **ARS Public Websites**
  The ARS Public Websites contains publicly available data. There are no PII risks.

- **NAL Azure Applications**
  The NAL Azure Applications contains publicly available data. There are no PII risks.
- **GRIN Azure Applications**
  The GRIN Azure Applications contains publicly available data. There are no PII risks.
  .

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

ARIS Applications

The information is used strictly for the unique identification of personnel. SSN is used by limited and authorized Human Resource (HR) Specialists that are responsible for collecting and reviewing personnel data from across REE and performing quality checks on the data. In performing quality checks, HR must verify employee personnel data pertaining to personnel actions including appraisals and awards against data in the National Finance Center. The primary purpose of using SSN is to properly identify the employee. Many employees have similar names and the use of SSN enables HR to identify the correct employee for purposes of verifying the employee regarding the personnel action (performance appraisal and awards management). Personnel files also must be uploaded into the employee's electronic Official Personnel File (eOPF). The SSN is required to upload the employee's package into the eOPF. The information is used only by offices and employees who have a need for the information in the performance of their official duties.

NAL, GRIN, and ARS public websites
No privacy data is present.

2.2 What types of tools are used to analyze data and what type of data may be produced?

N/A - ARIS does not use any type of tools to analyze PII data. No PII data is "produced". PII data is not manipulated.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

ARIS Applications: The system does not use any commercial or publicly available data.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

ARIS Applications: Only authorized personnel are given access to the system based on need to know and least privilege principles. Authentication is provided by USDA eAuthentication/LincPass access to privileged users only and data access is limited to need-to-know basis controlled by database accounts and roles. We are in the process of adding additional controls.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 How long is information retained?

The information is stored and maintained based on federal government data retention policies and NARA general records schedule 4.2 or ARS NARA approved retention schedule.

3.2 Has the retention period been approved by the component records officer and the National Archives and Records Administration (NARA)?

The retention period follows the ARS and NARA records management policy.

3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

Given the length of time data is retained within the system, the agency recognizes the risk of inadvertent privacy data disclosure. The risk is mitigated through a series of security measures built into the infrastructure and the system. Detailed description of implemented system security controls can be found in the system security plan. Application security controls are provided by USDA eAuthentication/LincPass access limited to authorized users only and data access is limited to “need to know” basis controlled by database accounts and roles.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the United States Department of Agriculture.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

N/A - ARIS does not transmit or share any PII data with any other internal USDA organization.

4.2 How is the information transmitted or disclosed?

N/A - ARIS does not transmit or disclose any PII with any internal USDA organization.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

ARIS does not share PII data with any other internal USDA organization.

To mitigate any risk of sharing PII data, only specific non-PII data elements are shared via manual processes that are controlled and data reviewed for correctness.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to USDA which includes Federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

ARIS does not share privacy data with external organizations.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it

covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of USDA.

No privacy data is shared outside the Department.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

Not applicable

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

Not applicable

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Does this system require a SORN and if so, please provide SORN name and URL.

GOVT-1 SORN (https://www.oge.gov/web/OGE.nsf/Resources/OGE+GOVT-1+SORN+(2019))

An ARS SORN is currently in progress.

6.2 Was notice provided to the individual prior to collection of information?

ARIS Applications doesn’t collect privacy information. The privacy data are imported from NFC.

6.3 Do individuals have the opportunity and/or right to decline to provide information?

Not applicable.

6.4 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

All PII data is maintained solely for the unique identification of personnel and is accessible only to authorized users with a need to know in the performance of their official duties.

6.5 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

The system displays a login banner when entering the system and users must acknowledge and consent to all information on the computer system may being intercepted, recorded, read, copied, and disclosed by and to authorized personnel for official purposes. All PII data is maintained solely for the unique identification of personnel and is accessible only to authorized users with a need to know in the performance of their official duties.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

ARS Azure doesn't collect sensitive PII. Users need to contact the original source (Human Resources/NFC) to gain access to their information or to request changes.

7.1 What are the procedures that allow individuals to gain access to their information?

ARS Azure doesn't collect sensitive PII. Users need to contact the original source (Human Resources/NFC) to gain access to their information or to request changes.

7.2 What are the procedures for correcting inaccurate or erroneous information?

ARS Azure doesn't collect sensitive PII. Users need to contact the original source (Human Resources/NFC) to gain access to their information or to request changes.

7.3 How are individuals notified of the procedures for correcting their information?

ARS Azure doesn’t collect sensitive PII. Users need to contact the original source (Human Resources/NFC) to gain access to their information or to request changes.

7.4 If no formal redress is provided, what alternatives are available to the individual?

Employees have formal lines of communication with their human resources representative and can request access to and correct their information when necessary.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

Employees have access to their information at the original source (Human Resources/NFC), and can request change/correction of their information when necessary as part of regular Human Resources activities. There is no identified risk.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system and are they documented?

USDA user accounts are managed in accordance with applicable USDA and ARS account management policies and procedures. Information system users are authenticated against the USDA eAuthentication and Oracle database and each user account is specific to a particular user. System, guest, anonymous, and other generic accounts, that are not specific to particular users, are prohibited.

The system owner assigns responsibilities to specific parties, and specific actions are defined to ensure that information system accounts are managed correctly. The process of management of the information system accounts including establishing, activating, modifying, reviewing, and locking, disabling, or deleting accounts is enforced through the use of online REE-235 and/or REE-236 forms. Before IT specialists can perform any account management action, the user's supervisor has to initiate and approve the request for account management event. The request is forwarded to IT specialists for final action. The system owner or their delegate maintains records of account management actions to document that account management actions are being performed in accordance with specific procedures. System account administrators regularly review information system accounts to ensure that continued account access is necessary. The information system automatically locks, disables, or deletes inactive accounts after 60 days of inactivity through OCIO CEC user account procedures.

8.2 Will Department contractors have access to the system?

USDA contractors have access to the system and the same rules stated in 8.1 apply.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

All information system users are required to take mandatory security awareness training before being granted access to the system and at least annually thereafter.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

The system has obtained its first ATO on 3/28/2022.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

The system is configured in accordance with the ARS Guidance on Audit Trails Management - the formal, documented audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; as well as formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.
All sessions are encrypted, and sensitive PII is being both encrypted and masked.

8.6 <u>Privacy Impact Analysis</u>: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

ARS institutes the best industry practices for safeguarding PII and FIPS 199. All sessions are encrypted, and sensitive PII is being masked.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware and other technology.

9.1 What type of project is the program or system?

The ARIS application is comprised of a set of in-house developed web based applications (developed in Oracle's Reports and Forms Developer Suite 12c) and Oracle's Relational Database (Oracle RDBMS version 12c). The system is cloud based, and the cloud platform is FEDRAMP certified.

9.2 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

No. The system does not utilize any technologies that would raise privacy concerns. The cloud platform is FEDRAMP certified.

Section 10.0 Third Party Websites/Applications

The following questions are directed at critically analyzing the privacy impact of using third party websites and/or applications.

10.1 Has the System Owner (SO) and/or Information Systems Security Program Manager (ISSPM) reviewed Office of Management and Budget (OMB) memorandums M-10-22 "Guidance for Online Use of Web Measurement and Customization Technology" and M-10-23 "Guidance for Agency Use of Third-Party Websites and Applications"?

Yes.

10.2 What is the specific purpose of the agency's use of 3rd party websites and/or applications?

The ARS Azure Applications use WebTrends (ARS public websites), Google Analytics (NAL Azure Applications) and DAP analytics (all public facing web-sites), which fall within the appropriate use and prohibitions of OMB Memoranda M-10-22. These are Tier 2 multi-session web measurement technologies that do not collect any PII. The information is enabled by the user-session cookie technology and users can elect to opt-out of the data collection by turning cookies off within their browser settings. We are stating that information appropriately under the USDA Privacy Policy that is included on our Policy Statement page.
Source code is managed through private repositories in github.com, access is managed and vetted by the repository owners and reviewed annually. Privacy data, passwords or other account information are not included in the source code repositories.

10.3 What personally identifiable information (PII) will become available through the agency's use of 3rd party websites and/or applications.

No PII is available through 3rd party websites/applications.

10.4 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be used?

Not applicable.

10.5 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be maintained and secured?

Not applicable

10.6 Is the PII that becomes available through the agency's use of 3rd party websites and/or applications purged periodically?

Not applicable.

10.7 Who will have access to PII that becomes available through the agency's use of 3rd party websites and/or applications?

Not applicable.

10.8 With whom will the PII that becomes available through the agency's use of 3rd party websites and/or applications be shared - either internally or externally?

Not applicable.

10.9 Will the activities involving the PII that becomes available through the agency's use of 3rd party websites and/or applications require either the creation or modification of a system of records notice (SORN)?

Not applicable.

10.10 Does the system use web measurement and customization technology?

The ARS Azure Applications use WebTrends (ARS public websites), Google Analytics (NAL Azure Applications) and DAP analytics (all public facing web-sites), which fall within the appropriate use and prohibitions of OMB Memoranda M-10-22. These are Tier 2 multi-session web measurement technologies that do not collect any PII. The information is enabled by the user-session cookie technology and users can elect to opt-out of the data collection by turning cookies off within their browser settings. We are stating that information appropriately under the USDA Privacy Policy that is included on our Policy Statement page.

If so, is the system and procedures reviewed annually to demonstrate compliance to OMB M-10-23?

Yes.

10.11 Does the system allow users to either decline to opt-in or decide to opt-out of all uses of web measurement and customization technology?

The information is enabled by the user-session cookie technology and users can elect to opt-out of the data collection by turning cookies off within their browser settings.

If so, does the agency provide the public with alternatives for acquiring comparable information and services?

The information is enabled by the user-session cookie technology and users can elect to opt-out of the data collection by turning cookies off within their browser settings.