Touchpoints

Privacy Impact Assessment

October 4, 2019

POINT *of* CONTACT

Richard Speidel

gsa.privacyact@gsa.gov

Chief Privacy Officer
GSA IT
1800 F Street NW
Washington, DC 20405

Table of contents

Document purpose

This document contains important details about *Touchpoints.* The Technology Transformation Service's Office of Products and Programs may, in the course of *Feedback Analytics*, collect personally identifiable information ("PII") about the people who use such products and services. PII is any information[1] that can be used to

distinguish or trace an individual's identity like a name, address, or place and date of birth.

GSA uses Privacy Impact Assessments (PIAs) to explain how it collects, uses, secures, and destroys information in ways that protect privacy. This PIA is comprised of sections that reflect GSA's privacy policy and program goals. The sections also align to the Fair Information Practice Principles ("FIPPs"), a set of eight precepts that are codified in the Privacy Act of 1974.[2]

For the purposes of this document, "customers" refers to federal agencies utilizing Touchpoints for collecting user feedback on public services, and "users" refers to members of the public.

System, Application or Project

Touchpoints

System, application or project includes information about

Federal employees, contractors and members of the public that use Federal digital products or services.

System, application or project includes

- **Survey data** is data such as voluntarily submitted name, contact information (for example, telephone number or email address), reason for visiting the digital product or service, and customer feedback on a public service. When necessary, this may also include demographic information such as age range, education level, language, profession, occupation, etc.
- **Administrative metadata** is data indirectly collected as a result of the survey (for example, the web form) through which a respondent indicates their interest in survey participation. It may include data such as timestamp, operating system, referrer, and user-agent (browser).

Overview

Touchpoints provides federal agency customers a no--cost, no-procurement way to collect user feedback for the purpose of improving the Customer Experience (CX) while using federal government websites and other digital services. while leveraging several available efficiencies for easing regulatory burden (e.g. expediting the PRA approval process for customer experience feedback via a GSA-managed generic PRA clearance).

Touchpoints helps streamline the gathering and reporting of feedback data for the purposes of improving customer experience and public service delivery.

GSA's work developing Touchpoints is done under the following authorities or Executive Orders:

- **Executive Order 13571**, Section 2B, which directs agencies to "establish mechanisms to solicit customer feedback on government services and use such feedback regularly to make service improvements". GSA's collection of contact information (if requested) is authorized by the E-Government Act of 2002 (P.L. 107-347, 44 USC § 3501).
- **2018 OMB Circular A-11, Section 280**: compliance for High Impact Service Providers participating in Cross Agency Priority Goal 4: Customer Experience.
- **21st Century IDEA Act** (2018)
- **Customer Experience CAP Goal**, GPRA (2013-2017, 2018-2020)
- **Policies for Federal Agency Public Websites & Digital Services** (M-17-06, 2016)

Touchpoints is launching with a limited number of form templates, in which fields requesting PII are included only if a partner agency identifies a business need. For example, when a partner agency seeks to recruit users to participate in customer research, it must collect respondent contact information, e.g. (first name, email/phone number). Once submitted by a user, the data is available for the customer agency to access within Touchpoints or export as a CSV file for a period of up to 3 years, at which point GSA will destroy it per the following NARA-approved schedules:

- 352.2/011 – Publicly-posted Information (DAA-0352-2016-0001-0004) - 3 years
- 352.2/021 – Information Service Program Management Records (DAA-0352-2016-0001-0005) - 3 years

SECTION 1.0 PURPOSE OF COLLECTION

GSA states its purpose and legal authority before collecting PII.

1.1 Why is GSA collecting the information?

GSA offers Touchpoints as a service to any Federal agency seeking feedback from the public on digital services. In order to provide this service, Touchpoints can collect contact information from survey respondents, and may also be used to manage and report on survey results. Any user that submits PII through surveys does so on an opt-in basis and is provided notice that PII is not required. Where a business need has been identified, each survey is designed to collect the minimum amount of PII required to achieve the customer agency's mission goal.

1.2 What legal authority and/or agreements allow GSA to collect the information?

GSA's work developing Touchpoints is done under the following authorities or Executive Orders:

- **Executive Order 13571**, Section 2B, which directs agencies to "establish mechanisms to solicit customer feedback on government services and use such feedback regularly to make service improvements". GSA's collection of contact information is authorized by the E-Government Act of 2002 (P.L. 107-347, 44 USC § 3501).
- **2018 OMB Circular A-11, Section 280**: compliance for High Impact Service Providers participating in Cross Agency Priority Goal 4: Customer Experience.
- **21st Century IDEA Act** (2018)
- **Customer Experience CAP Goal**, GPRA (2013-2017, 2018-2020)
- **Policies for Federal Agency Public Websites & Digital Services** (M-17-06, 2016)

1.3 Is the information searchable by a personal identifier, for example a name or Social Security Number? If so, what System of Records Notice(s) apply/applies to the information being collected?

Touchpoints information is not searchable by a personal identifier. Instead, each submitted form response is assigned a random numeric identifier in the system.

1.4. Has any information collection request (ICR) been submitted to or approved by the Office of Management and Budget (OMB)? If yes, provide the relevant names, OMB control numbers, and expiration dates.

ICRs for Touchpoints surveys are submitted to OIRA for each survey individually, on a rolling basis. For all forms other than the A-11 survey, that process is managed by the agency customer in coordination with their internal PRA desk. The A-11 survey instrument PRA approvals will be managed by Touchpoints' staff under a generic clearance held by GSA, in coordination with GSA's RegSec office, via a bespoke (for this purpose) process defined by OIRA:

Information Collection 3090-XXXX, Improving Customer Experience (A-11, Section 280, https://www.regulations.gov/document?D=GSA-GSA-2019-0001-0012

1.5. Has a records retention schedule been approved by the National Archives and Records Administration (NARA)? Explain how long and for what reason the information is retained.

In consultation with GSA's Senior Records Officer, the following schedules provide retention periods for Touchpoints' data:

- 352.2/011 - Publicly-posted Information (DAA-0352-2016-0001-0004) - 3 years
- 352.2/021 – Information Service Program Management Records (DAA-0352-2016-0001-0005) - 3 years

SECTION 2.0 OPENNESS AND TRANSPARENCY

GSA is open and transparent. It notifies individuals of the PII it collects and how it protects, uses and shares it. It provides straightforward ways for individuals to learn about how GSA handles PII.

2.1 Will individuals be given notice prior to the collection and/or sharing of personal information about themselves? If not, please explain.

All applicable survey instruments are required to have a valid OMB PRA Approval number, which requires notice of information collection be provided to the public in

advance of the collection, and throughout the duration the instrument is accessible for response.

All agency customer users of Touchpoints' administrative interface are subject to its published Terms of Service.

SECTION 3.0 DATA MINIMIZATION

GSA limits the collection of PII to what is needed to accomplish the stated purpose for its collection. GSA keeps PII only as long as needed to fulfill that purpose.

3.1 Whose information is included in the system, application or project?

Federal Employees, Contractors, Members of the public that attempt to receive public services, either online by visiting a website or application, in person, via phone, email or mail.

3.2 What PII will the system, application or project include?

Currently, Touchpoints has three form instrument “templates” - combinations of input fields designed for common customer experience evaluation purposes.

- **A-11 form template**: no PII is requested
- **Recruiter form template**: First Name, phone (optional), email address (optional)
- **Open text feedback form template**: a single multi-line text input, (no PII is requested or required)

3.3 Why is the collection and use of the PII necessary to the system, application or project?

Administrative User (AU) information in Touchpoints administrative interface consists solely of email address provided via Login.gov authentication.

Survey response information may also be directly collected from individuals participating in surveys. Links to surveys can be published to both Agency Customer web properties, are accessible at https://touchpoints.digital.gov, and may also be distributed by email to survey respondents. Limited, voluntarily-supplied PII may be collected (such as a first

name) as well as voluntary contact information (e.g., email address, telephone number) for the purpose of contacting the user to resolve customer service issues.

Additionally, users are warned not to submit sensitive personal information in-line on the survey interface itself.

3.4 Will the system, application or project create or aggregate new data about the individual? If so, how will this data be maintained and used?

Touchpoints does not include functionality to facilitate aggregating identifiable data about individuals from multiple sources to derive novel PII.

3.5 What protections exist to protect the consolidated data and prevent unauthorized access?

Touchpoints is scanned at regular interval for vulnerabilities in the information system and hosted applications, and when new vulnerabilities potentially affecting the system/applications are identified and reported, Feedback Analytics PMO staff analyzes vulnerability scan reports and results from security control assessments; remediates legitimate vulnerabilities within appropriate time periods relative to the severity of the finding.

CircleCI is a continuous integration tool used for running automated tests of the Touchpoints software. Snyk is a static code analysis tool used to scan Ruby and Javascript dependencies for vulnerabilities.

Additionally, Touchpoints participates in GSA’s Bug Bounty program.

3.6 Will the system monitor the public, GSA employees or contractors?

Touchpoints does not have the capability to locate or monitor individuals.

3.7 What kinds of report(s) can be produced on individuals?

While it does collect internet protocol addresses (IPs), the system does not monitor individuals and each agency can only access the comments submitted on its service/application.

3.8 Will the data included in any report(s) be de-identified? If so, what process(es) will be used to aggregate or de-identify the data?

Touchpoints does not have the capability to report on individuals. Each agency can access only the comments submitted on its service/application. An agency may download all comments to .csv file, but there is no native reporting capability.

SECTION 4.0 LIMITS ON USES AND SHARING OF INFORMATION

GSA publishes a notice about how it plans to use and share any PII it collects. GSA only shares PII in ways that are compatible with the notice or as stated in the Privacy Act.

4.1 Is the information in the system, application or project limited to only the information that is needed to carry out the purpose of the collection?

Agency Customers authenticate via Login.gov, which shares only that customer's email address and name with Touchpoints.

Users have the opportunity to decline to provide their personal data or to consent to particular uses of their information (e.g. requesting follow-up contact to resolve customer service issues).

4.2 Will GSA share any of the information with other individuals, Federal and/or state agencies, or private sector organizations? If so, how will GSA share the information?

GSA does not access and will not share Touchpoints information with anyone other than the agency the user submitted it to..

4.3 Is the information collected directly from the individual or is it taken from another source? If so, what is the other source(s)?

Survey respondents will generally submit information directly to Touchpoints. Some surveys may be administered verbally by customer agency staff holding a tablet computer at a service point of interaction (a "touch point") and submitted on the customer's behalf to Touchpoints, a TSA agent might ask travelers about their experience at airport security checkpoints, where participation is challenging as travelers' hands are full of baggage.

4.4 Will the system, application or project interact with other systems, applications or projects, either within or outside of GSA? If so, who, how and is a formal agreement(s) in place?

Touchpoints is hosted on Cloud.gov and utilizes Login.gov for multi-factor authentication of customers to the Administrative Interface. Cloud.gov is a direct contract/MOU between Cloud and the Feedback Analytics Project Management Office (PMO); while the Login.gov implementation is a "subcontract," part of a larger acquisition by the Office of Solutions within the Technology Transformation Services.

SECTION 5.0 DATA QUALITY AND INTEGRITY

GSA makes reasonable efforts to ensure that all PII it maintains is accurate, relevant, timely, and complete.

5.1 How will the information collected be verified for accuracy and completeness?

Since information submitted via Touchpoints is voluntary and subjective, information will not be verified for accuracy or completeness at this time.

SECTION 6.0 SECURITY

GSA protects PII from loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

6.1 Who or what will have access to the data in the system, application or project? What is the authorization process to gain access?

Feedback Analytics program staff and contractors have administrative access to Touchpoints data (e.g. access to repository where the form templates are stored and may escalate agency customer privileges).

Each customer agency designates staff to serve as Organization Manager(s), who has the ability to grant access to view and download their surveys and responses in Touchpoints. Agency customer staff users are granted access to only the data available for their

Organization (as determined by the Organization Manager). Agency customers are responsible for determining which of their staff may access and download data through Touchpoints as Service Managers or Submission Viewers.

Touchpoints User Roles and Privileges

Role	Authorized Privileges and Functions Performed
System Administrator	**Scope: System-wide** ● Can create an Organization ● Can create FormTemplates ● Can create PRA Contacts ● Can manage Container and its Tags and Triggers ● Can do everything an Organization Manager and Service Manager can do
Organization Manager	**Scope: Within an Organization** ● Can edit their Organization ● Can authorize an Organization Manager by editing an existing User in the same Organization as the Organization Manager ● Can authorize a Service Manager by adding a User to a Service ● Can do everything a Service Manager can do
Service Manager	**Scope: Related to a Service** ● Can authorize another Service Manager by adding a User to a Service ● Can create a Service ● Can create an Event ● Can create a Touchpoint ● Can create a Form based on a FormTemplate ● Can Flag a Submission ● Can Delete a Submission
Submission Viewer	**Scope: for specific Touchpoints this user has been added to as a Submission Viewer** ● Can view the assigned Touchpoint's Service ● Can view the assigned Touchpoint's Submissions ● Can Flag a Submission
Public User	● Can create a Submission for a Touchpoint

6.2 Has GSA completed a system security plan for the information system(s) or application?

Yes, GSA finalized the system security plan for Touchpoints on 8/18/2019.

6.3 How will the system or application be secured from a physical, technological, and managerial perspective?

Touchpoints enforces authorization via custom implemented roles and permissions. Access to resources is dependent upon a user's role and permissions; e.g. Organization Manager, Service Manager, or Submission Viewer.

Touchpoints maintains an automated test suite that includes "feature tests" (also known as "specs") that exercise the integrated application with a web browser, simulating a user's experience. This is a first-pass check for exceptions and system integration issues.

On an annual basis, an OWASP ZAP scan is performed in coordination with GSA IT.

Touchpoints monitors and controls communications at the external boundary of the system and at key internal boundaries within the system, implements subnetworks for publicly accessible system components that are logically separated from internal organizational networks, and connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

6.4 Are there mechanisms in place to identify suspected or confirmed security incidents and breaches of PII? If so, what are they?

Touchpoints is hosted by Cloud.gov, which monitors system activity and analytics and alerts application owners of any suspicious or anomalous traffic/patterns.

Touchpoints employs vulnerability scanning tools. Each code commit is scanned for vulnerabilities using Snyk, and GitHub (where source code is versioned) also sends alerts to staff based on known vulnerabilities. Weekly Nessus scans and monthly Netsparker scans are performed on the system, coordinated by Touchpoints' ISSO, SecOps and GSA IT.

SECTION 7.0 INDIVIDUAL PARTICIPATION

GSA provides individuals the ability to access their PII and to correct or amend it if it is inaccurate. If GSA exempts a system or program from access, amendment and other provisions of the Privacy Act, it notifies the public of that exemption.

7.1 What opportunities are available for individuals to consent to uses, decline to provide information or opt out of providing information? If no opportunities exist to consent, decline or opt out, please explain.

Participation in Touchpoints surveys is voluntary. A person's responses (or lack thereof) can in no way affect that person's eligibility for or access to any government benefit, service, or position.

With the exception of contact information (name, work or personal email address and phone number) collected with the user's consent for the purpose of following up with a user about their feedback, response data is not associated with identifiable information about the respondent.

7.2 What procedures allow individuals to access their information?

Individuals can access and review their survey responses up until they "submit" the form. The system does not permit individuals to update or change previously-submitted survey responses.

Agency customer Organization Managers are granted access to their Organization by Feedback Analytics program staff. Organization Managers are responsible for determining access permissions for their Touchpoints surveys.

7.3 Can individuals amend information about themselves? If so, how?

No. Touchpoints does not store survey response data associated with the survey respondent such that it is searchable within the system or editable after submission.

SECTION 8.0 AWARENESS AND TRAINING

GSA trains its personnel to handle and protect PII properly.

8.1 Describe what privacy training is provided to users, either generally or specifically relevant to the system, application or project.

All Feedback Analytics Program staff with Administrator (full privilege) rights to access Touchpoints have undergone GSA's annual Privacy and Security training.

SECTION 9.0 ACCOUNTABILITY AND AUDITING

GSA's Privacy Program is designed to make the agency accountable for complying with the Fair Information Practice Principles. GSA regularly checks that it is meeting the requirements and takes appropriate action if it is not.

9.1 How does the system, application or project ensure that the information is used in accordance with the stated practices in this PIA?

The Feedback Analytics program will conduct biannual reviews of authorized Agency Customer accounts, requesting via email that each Organization Manager reviews users with access to their surveys and survey results in Touchpoints, and remove any out-of-date or otherwise invalid account access.

---

[1] OMB Memorandum *Preparing for and Responding to a Breach of Personally Identifiable Information* (OMB M-17-12) defines PII as: "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 memorandum notes that "because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad."

[2] Privacy Act of 1974, 5 U.S.C. § 552a, as amended.

APPENDIX A:
TOUCHPOINTS PRIVACY RISKS AND MITIGATIONS

For the purposes of this document, "customers" refers to federal agencies utilizing Touchpoints for collecting user feedback on public services, and "users" refers to members of the public.

Risk	Mitigation
Unauthorized information collection	● Feedback Analytics Program manager publishes privacy impact assessment ● Training for Touchpoints' agency customers ○ Use of approved sampling protocols ○ Structured information collections (PRA) ● Training/in-application affordances for Touchpoints users: ○ Data minimization: Touchpoints collects minimal metadata with submissions such as IP address, browser name, referrer in addition to survey response ○ Protections against unauthorized information collection: instructions and notices to users, limiting the use of open text fields, help text reminding users not to enter sensitive information in survey fields.
Inappropriate information collection	● Training for Touchpoints' agency customers ○ Customers will be required to explain the nature and purpose of their information collection from survey respondents as part

	of the PRA approval process for new form instruments
Inappropriate information disclosure (e.g. a survey respondent includes their social security number in a free-text response field)	● Training for Touchpoints' agency customers ○ Appropriate information disclosures on form instruments ○ Ensuring the OMB PRA clearance under which collection occurs allows for publication or release before distributing, publishing, or otherwise sharing ○ De-identification as a risk mitigation ○ How to flag inappropriate submissions in Touchpoints admin interface to prevent download of unnecessary sensitive info by customer
Misuse of information	● Training for Touchpoints' agency customers ○ Partner agency administrative user data is never shared. ○ Access to survey response data in Touchpoints is shared on a need-to-know basis, as determined by agency's Organization Manager. ○ Customers are informed of the application of records retention rules for all Touchpoints records (currently via Touchpoints' Terms of Service).
Use limitation	● Data submitted by survey respondents is hosted and stored by GSA on behalf of Agency Customers. Submission data may be viewed in a simple tabular format

	within the Touchpoints Administrative Interface, or downloaded for analysis via common tools, e.g. Excel or Tableau. Data exports are available via download only, not as email attachments. Data exports are recorded in Touchpoints' application logs for audit purposes.