Version Number: 01-2017

U.S. Department of Commerce
Bureau of the Census

Privacy Threshold Analysis
for the
MobileUsabilityLab

U.S. Department of Commerce Privacy Threshold Analysis

Bureau of the Census/ MobileUsabilityLab

Unique Project Identifier: [Number]

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: *Provide a general description of the information system in a way that a non-technical person can understand.*

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

The system, MobileUsabilityLab (MULab), is a suite of native mobile apps running on iOS on three designated Census-owned-and-certified iPhones (6s). MULab will be used for conducting usability experiments on the user interface of mobile questionnaires and of data dissemination apps. Each app is designed to meet the requirements for a particular experiment, and is a relatively simple piece of software that implements a limited number of functionalities, mainly data collection and storage. The test environment for the system is the Census-owned-and-certified iPhone. The testing effort will ensure that the functionality and usability of the mobile apps meet the design specifications. Test data will consist of general information, specifically user performance data that are not in the category of Personal Identity and Authentication.

The MULab system consists of 32 experiment apps. Six of the experiments are designed to collect PII data, while the rest of the experiments do not collect PII data. There will be no additional PII-data collecting experiments to be added to the MULab system in the future. **The purpose for collecting PII is to assess the effect of user interface design on the quality of PII the respondent enter in responding to an official survey (e.g., 2020 Census). This type of assessment is mission-critical and there is no alternative to using PII. To minimize the potential impact of PII retention on privacy protection, PII data will be destroyed immediately upon the completion of data analysis or 12 months from the PII is collected, whichever comes first.** The data will be encrypted in compliance with FIPS 140-2 standards. Data collected by a particular experiment app will not be accessible by other apps on the same iPhone. Data collected in an iPhone during testing will be transferred from the iPhone to a Census-owned-and-certified MacBook laptop computer via a cable connection. Data on the Census-owned-and-certified MacBook laptop computer will be transferred to CSM shared

storage via cable connection or Census production WiFi network. CSM shared storage is covered by CSvD CEN16; and the production WiFi is covered by the Telecommunications Office (TCO) CEN01. Access to the information is protected with an access control list. Only authorized personnel on the access control list can access the information.

a) Whether it is a general support system, major application, or other type of system

The system is a research software that supports research on mobile devices user interface usability for survey operations.

b) System location

MULab will operate on three (3) designated Census-owned-and-certified iPhones (6s).

c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

MULab is a standalone system. Wireless technologies are not used in MULab, and there is no networking functionality within the MULab. The wireless and Wi-Fi Network communication capability on the iPhone is deactivated. This measure ensures that no data inside a Census-approved-and-certified iPhone can be transmitted to an unsecure media via wireless or Wi-Fi.

d) The purpose that the system is designed to serve

MULab is designed to conduct usability research on mobile device user interface for survey operations.

e) The way the system operates to achieve the purpose

In a usability research experiment, an authorized Census-Bureau-employee researcher operates the MULab system to conduct the experiment and to collect data entered by the research participant during the experiment session.

f) A general description of the type of information collected, maintained, use, or disseminated by the system

The information collected by the system is (1) responses to survey questions, (2) user actions during task performance, e.g., time taken to answer a survey question, errors made in data entry, etc.

g) Identify individuals who have access to information on the system

Census Bureau employees who are involved in the research that uses the information collected by the system

h) How information in the system is retrieved by the user

Only the system administrator can retrieve the information following the protocol: (1) log in Census-owned-and-certified iPhone with touch ID, (2) connect the iPhone to the Census-owned-and-certified MacBook with a cable, (3) transfer the information from the iPhone to the MacBook through the cable connection, and then transfer the information from the MacBook to designated Census network storage. Users involved in the research can log in Census network and retrieve relevant information from the designated Census network storage. The designated Census network storage is protected by an access control list.

i) How information is transmitted to and from the system

No information is transmitted to and from the system when the system is in operation. When the system is not in operation, information in the system can be transferred following the protocol: (1) log in Census-owned-and-certified iPhone with touch ID, (2) connect the iPhone to the Census-owned-and-certified MacBook with a cable, (3) transfer the information from the iPhone to the MacBook through the cable connection, and then transfer the information from the MacBook to designated Census network storage. Users involved in the research can log in Census network and retrieve relevant information from the designated Census network storage. The designated Census network storage is protected by an access control list.

Questionnaire:

1. What is the status of this information system?

__x__ This is a new information system. *Continue to answer questions and complete certification.*

____ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System		f. Commercial Sources		i. Alteration in Character	

Management Changes				of Data	
j. Other changes that create new privacy risks (specify):					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

____ Yes. *Please describe the activities which may raise privacy concerns.*

__x__ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

____ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

____ Companies
____ Other business entities

__x__ No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

__x__ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

____ DOC employees
____ Contractors working on behalf of DOC
_x___ Members of the public

____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

__x__ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

__x__ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

__x__ I certify the criteria implied by one or more of the questions above **apply** to the MULab and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the [IT SYSTEM NAME] and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of System Owner (SO): Paul Beatty

Signature of ISSO or SO: Paul C Beatty Date: 5/24/18

Name of Chief Information Security Officer (CISO): Tim Ruland

Signature of CISO: Tim Ruland acting for CISO Date: 5/24/18

Name of Authorizing Official (AO): Kevin Smith

Signature of AO: Kevin Smith Date: 5/24/18

Name of Authorizing Official (AO): John Eltinge

Signature of AO: Date: 5/24/2018

Name of Bureau Privacy Officer (BPO): Byron Crenshaw

Signature of BPO: Byron Crenshaw for Date: 5/24/18