Version Number: 01-2017

U.S. Department of Commerce
Bureau of the Census

Privacy Impact Assessment
for the
MobileUsabilityLab

Reviewed by: _____, Bureau Chief Privacy Officer

☑ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

CATRINA PURVIS

Digitally signed by CATRINA PURVIS
DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=CATRINA PURVIS, 0.9.2342.19200300.100.1.1=13001002875743
Date: 2018.06.21 10:12:16 -04'00'

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
Bureau of the Census/MobileUsabilityLab

Unique Project Identifier: [Number]

Introduction: System Description

Provide a description of the system that addresses the following elements:
The response must be written in plain language and be as comprehensive as necessary to describe the system.

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 piece of 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 way the system operates to achieve the purpose(s) identified in Section 4

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

e) 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.

f) 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.

(g) Any information sharing conducted by the system

The MobileUsabilityLab operates as a stand-alone system on an iPhone. Information collected is transferred to a Census-owned-and-certified MacBook via a cable. The information is then transferred to a secured and access-restricted storage server within Census Bureau network, via a secure connection within the Census Bureau's headquarters.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

13 U.S.C., Chapter 5, 6, 8(b), 131, 141, 161, 182, and 193

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

Moderate

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

__x_ This is a new information system.
____ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

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 Management Changes		f. Commercial Sources		i. Alteration in Character 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.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*		e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License		j. Financial Account	
c. Employer ID		g. Passport		k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	x	g. Date of Birth	x	m. Religion	
b. Maiden Name		h. Place of Birth	x	n. Financial Information	
c. Alias		i. Home Address	x	o. Medical Information	
d. Gender	x	j. Telephone Number	x	p. Military Service	
e. Age	x	k. Email Address	x	q. Physical Characteristics	
f. Race/Ethnicity	x	l. Education	x	r. Mother's Maiden Name	
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	x	d. Telephone Number		g. Salary	
b. Job Title		e. Email Address		h. Work History	
c. Work Address		f. Business Associates			
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID		c. Date/Time of Access		e. ID Files Accessed	
b. IP Address		d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains

In Person*	x	Hard Copy: Mail/Fax		Online	
Telephone		Email			
Other (specify): * The participant is physically given the cellphone to enter their data into MULab.					

Government Sources					
Within the Bureau		Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify):					

Non-government Sources					
Public Organizations		Private Sector		Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

2.3 Describe how the accuracy of the information in the system is ensured.

The accuracy of the information in the system is ensured through storing the information verbatim without any manipulation.

2.4 Is the information covered by the Paperwork Reduction Act?

x	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. 0607-0725
	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

x	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

x	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program		For administering human resources programs	
For administrative matters		To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): To improve the accuracy of PII provided by the public in response to official surveys, and consequently to reduce survey measurement error.			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

The PII will be used in usability research on mobile applications of survey data collection. The purpose of research is to improve the experience of the members of the public in completing government surveys and to reduce measurement error and response error in official surveys. In order to simulate respondent's experience of survey completion, some experiments in MULab have to include questions involving PII. The PII identified in Section 2.1 of this document is in reference to a member of the public.

The ultimate goal of MULab is to improve online official surveys that are taken via a smartphone.

5.2 Describe any potential threats to privacy as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

A potential threat to privacy as a result of the use of the information is unintentional disclosure of the information. To minimize the threat, the operating unit has placed the following controls:

(1) All government staff using the information receive mandatory training on PII and Title 13 data stewardship.
(2) All information is de-identified and encrypted in compliance with FIPS 140-2.
(3) All information stays at any moment on Census secure media.
(4) Information retention complies the GRS 3.1 and 3.2

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	x		
DOC bureaus			
Federal agencies			
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

	The PII in the system will not be shared.

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

x	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: MULab does not have a direct connection with other Census Bureau IT systems. However, the data collected by MULab will be transferred to a Census-owned MacBook via a cable. The data will then be transferred to a Census Bureau shared drive on Census Bureau Servers (CEN16) via a secure connection within the Census Bureau's headquarters. The Census Bureau uses a multitude of security controls mandated by the Federal Information Security Management Act of 2002 (FISMA) and various other regulatory control frameworks including the National Institute of Standards and Technology (NIST) special publication 800 series. These security controls include, but are not limited to the use of mandatory HTTPS for public facing websites, access controls, anti-virus solutions, enterprise auditing/monitoring, encryption of data at rest, and various physical controls at Census facilities that house Information Technology systems. The Census Bureau also deploys an enterprise Data Loss Protection (DLP) solution as well.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	x
Contractors			
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or

disseminated by the system. *(Check all that apply.)*

x	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
x	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: https://www.census.gov/about/policies/privacy/privacy-policy.html _____.	
x	Yes, notice is provided by other means.	Specify how: Notice is also provided on a separate document, titled Privacy Act Statement, given to the participant.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

x	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: The individuals can refuse to participate, verbally or in writing to the Census employee, before or during the data collection activities at any time.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

x	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: The individuals will have an opportunity to consent to the collection of information for research purposes only. However, the individual does not have the authority to determine how their information is used in research.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

x	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: The individuals will be given the contact information of the Census Bureau usability group, and can contact the usability group at any time to update their PII.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

x	All users signed a confidentiality agreement or non-disclosure agreement.
x	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
x	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.

x	Access to the PII/BII is restricted to authorized personnel only.
	Access to the PII/BII is being monitored, tracked, or recorded.
	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): _____ ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
x	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
x	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
	A security assessment report has been reviewed for the supporting information system and it has been determined that there are no additional privacy risks.
	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
x	Other (specify): An assessment was completed by OIS to validate that the appropriate administrative and technological controls are implemented in the system and that the inadequate functions are appropriately disabled.
x	There is no plan to obtain an Authority to Operate (ATO) this system; it is strictly for testing purposes. MULab has a current, signed and approved Authority to Test (ATT)

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

The technologies used to protect PII on the MULab system are:

1) Implement FIPS 140-2 data encryption.
2) Make no connection to and consequently no data transmission to/from any IT systems outside MULab, except the only ad-hoc connection for data transfer as described in 3).
3) Manually transfer data from the MULab data storage on the iPhone to Census Bureau's secure data storage via a temporary cable connection on as-needed basis by authorized Census personnel.
4) Implement the Census Mobile Device Management (MDM) policy to enforce locking the iPhone after 1 minute, and requires user authentication to unlock the phone.
5) Use the Census MDM to allow the Census Bureau to remotely wipe the data on the iPhone in the event that the device is lost or stolen.
6) Require the user to use the device-provided and Census-approved authentication mechanism to operate MULab.
7) Implement data-element level audit trail.

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C.

§ 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

x	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: COMMERCE/CENSUS-3- Special Censuses, Surveys, and Other Studies- http://osec.doc.gov/opog/PrivacyAct/SORNs/census-3.html COMMERCE/CENSUS-4- Economic Survey Collection- http://osec.doc.gov/opog/PrivacyAct/SORNs/census-4.html COMMERCE/CENSUS-5- Decennial Census Program- http://osec.doc.gov/opog/PrivacyAct/SORNs/census-5.html COMMERCE/CENSUS-7- Special Censuses of Population Conducted for State and Local Government- http://osec.doc.gov/opog/PrivacyAct/SORNs/census-7.html
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

x	There is an approved record control schedule. Provide the name of the record control schedule: GRS 3.1 and 3.2
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
x	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding		Overwriting	
Degaussing		Deleting	x
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
x	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

x	Identifiability	Provide explanation: Combined data elements uniquely and directly identify individuals.
x	Quantity of PII	Provide explanation: A serious or substantial number of individuals affected by loss, theft, or compromise. Serious collective harm to individuals, harm to the organization's reputation, or cost to the organization in addressing a breach.
x	Data Field Sensitivity	Provide explanation: Data fields, alone or in combination, may be relevant in some other contexts and may, in those contexts, make the individual or organization vulnerable to harms, such as identity theft, embarrassment, loss of trust, or costs.
x	Context of Use	Provide explanation: Disclosure of the PII/BII in this IT system or the PII/BII itself may result harm to the individual or organization.
x	Obligation to Protect Confidentiality	Provide explanation: 13 U.S.C. § 9 requires that data collected by the Census Bureau in its surveys, including the Decennial Censuses, shall remain confidential.
x	Access to and Location of PII	Provide explanation: PII/BII is located on devices/servers controlled by the Census Bureau. Access is limited to certain populations of the Census Bureau's workforce and limited to Special Sworn Status individuals. Access is only allowed by organization-owned devices outside of the physical locations and data must be transferred via secured connections.
	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

There are no additional potential threats to privacy.

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
x	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
x	No, the conduct of this PIA does not result in any required technology changes.