Federal Trade Commission
Privacy Impact Assessment
for the: Mobile/Internet Lab

May 2014

The Federal Trade Commission's (FTC) Bureau of Consumer Protection (BCP) protects consumers from a variety of fraudulent, deceptive, and unfair practices in the marketplace, including identity theft, telemarketing fraud, Internet fraud, and consumer credit issues. To further its consumer protection mission, the FTC brings civil and administrative law enforcement actions to enforce its laws and provides consumer and business education to enable the public to avoid common harms. The FTC works to ensure that consumers have accurate information to make purchasing decisions and have confidence in the traditional and electronic marketplaces.

BCP's consumer protection-related activities include collecting and analyzing consumer complaints, investigating individual companies, administrative and federal court litigation, rulemaking, educating consumers and businesses, and operating consumer protection programs. Increasingly, these activities require access to information and services available through the Internet and in the mobile marketplace.

To support BCP's growing need for Internet-related information and services and for familiarity with mobile devices and applications, BCP created a "Mobile/Internet Lab" (MIL). The MIL comprises a main facility in Washington, D.C., as well as eight satellite locations (one in each of the FTC's regional offices).

BCP's Division of Planning and Information (DPI) manages the MIL and, together with the FTC's Office of the Chief Information Officer (OCIO), maintains the MIL.

The MIL is primarily used by law enforcers (e.g., attorneys, investigators, paralegals) in the FTC's Bureau of Consumer Protection, and by technologists in DPI. On occasion, the MIL may also be used by authorized law enforcement partners, e.g., the Department of Justice, staff in other FTC offices, e.g., the FTC's Bureau of Competition (BC), the Office of General Counsel (OGC), the Office of the Inspector General (OIG), the Office of International Affairs (OIA), the Bureau of Economics (BE), and OCIO; and by experts or contractors retained by the FTC on particular matters. Individuals in these various groups are referred to in this Privacy Impact Assessment (PIA) as users.

1 System Overview

BCP's Mobile/Internet Lab comprises various customized commercial off-the-shelf (COTS) hardware and software tools and resources. The MIL provides users with secure and anonymous access to the Internet via computers and mobile devices, and to tools to investigate, capture, and preserve digital content. The MIL does not solicit information directly from individuals, except in limited undercover situations. Rather, the tools in the MIL allow users to preserve content that is directly available to the public through the Internet.

The MIL also provides users with access to the Internet via multiple high-speed connections, which are logically and physically isolated from the FTC's production network.

The MIL provides users with access to a select group of pre-approved mobile devices that can connect to the Internet through the MIL's dedicated wireless access point, external Wi-Fi hotspots, or commercial carrier networks, i.e., 3G, 4G. These mobile devices include smart phones, tablets, and other Wi-Fi capable devices purchased specifically for use by the MIL. Users may check out mobile devices and use them for pre-approved purposes outside the MIL. Device check in/out is administered by MIL staff, who track all device usage.

Because of the investigative and law enforcement mission of the MIL, software, mobile devices, and Internet services are all registered anonymously and are not readily traceable to the FTC by the target(s). This anonymity allows users to perform research and conduct investigations without being detected as FTC staff or users. In addition, because the MIL devices are prohibited from connecting to the FTC's production (computer) network, they can be used to access sites which may be blocked by FTC web filters; to make use of apps or software not available on FTC hardware; and to investigate computer viruses and other forms of malware without risk of contaminating the FTC's production network and devices. In this way, MIL users are able to simulate the day-to-day consumer experience.

The MIL provides users with the hardware and software they need to perform investigations and capture digital content, including mobile devices, computers, servers, networking devices, printers, scanners, cameras, and various software products. These tools provide users with the ability to capture content in the following formats: 1) printed/hardcopy; 2) static and dynamic digital images and recordings (e.g., screen shots); and 3) raw digital content (e.g., electronic copy of website or mobile app code or audio content/files). The tools available in the MIL also provide users with the ability to analyze Internet protocol and website registration information; network traffic, viruses, spyware, and other forms of malware; cookies, beacons, computer registry information, and other forms of web-tracking technologies; as well as emerging Internet and mobile technologies and threats. The MIL also provides users with tools for creating undercover email addresses and web sites, as well as tools for organizing and presenting the information that is obtained using MIL resources.

Information that users may obtain while using MIL resources is not systematically saved or stored within the MIL. Rather, it is either removed and preserved by users for use in their investigations, or it is destroyed, deleted, or overwritten as part of regular MIL maintenance procedures.

Administrative information concerning user activities within the MIL is also collected and maintained for a limited period of time for security and auditing purposes.

2 Information Collected and Stored within the System

.1 What information is to be collected, used, disseminated, or maintained by the system?

The MIL is used to view, collect, and when appropriate, preserve information that is available through the Internet or mobile devices. As stated previously, the MIL does not solicit information directly from individuals, except in limited undercover situations.

Information that is collected using the MIL may include content that is available to the public for free (with or without registering as a user) or offered to the public through paid/premium services on the Internet or in the mobile marketplace. This information may include mobile applications or website content, including personally identifiable information (PII) that may be available on the site, as well as usage data and statistics, IP addresses and domain registration and ownership information. PII collected in the MIL may include names, addresses, phone numbers, email addresses, and any other PII posted on a web site, included in the code or contact information of an app, or otherwise publicly available on the Internet or mobile marketplace.

In addition, access and event log data about internal MIL user activities, including the MIL user's name, phone number, organization code, time and date of entry and exit, mobile device usage, and network traffic are collected and maintained for management, security, and auditing purposes.

.2 What are the sources of the information in the system?

Information, including any PII posted by an individual target of an investigation or by a third party, is collected directly from the Internet or mobile marketplace and may include content freely available to consumers, content available to registered site members, and content that is only offered through paid/premium services. The MIL does not solicit information directly from individuals, except in limited undercover situations.

Administrative information about internal MIL user activities is collected directly from authorized FTC MIL users at the time of use.

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

Information is collected to support the FTC's law enforcement mission as discussed Section 1, above. For example, the MIL may be used to collect and preserve web pages or mobile content containing fraudulent or misleading information provided by targets of FTC investigations. Targets frequently change the content of their websites and apps, and collection and preservation of this information is, therefore, critical to proving that a fraudulent or misleading statement appeared on a particular web page or app on a particular day.

MIL activity and usage information is collected for administrative and security purposes. Access and event logs track who uses the facilities and ensure that such use is appropriate.

.4 **How is the information collected?**

Information is collected in the MIL with the tools described in Section 2, above. Information collection must be initiated by users. The MIL does not engage in automated scanning, collection, or similar passive data collection or data analysis activities.

MIL activity and usage information is collected through system event and device usage logs. In addition, the Washington, D.C. MIL collects physical access information by logging key card access to the MIL (e.g., time, date, and identity of FTC MIL user entering the facility).

.5 **How will the information be checked for accuracy and timeliness (currency)?**

The information collected by users will not be systematically checked for accuracy and timeliness. Information available on the Internet and mobile marketplace is subject to frequent/continuous change. Therefore, information that is collected by users is considered an accurate representation of the content as of the time it was collected.

MIL administrative information is actively monitored by MIL staff and is subject to review and audits by OCIO's Operations Assurance branch (OA).

.6 **Is the system using technologies in ways that the FTC has not previously employed (e.g., monitoring software, Smart Cards, etc.)? If so, how does the use of this technology affect individuals' privacy?**

The MIL uses mobile devices, apps, and tools to access the mobile marketplace for investigative purposes, as discussed in Section 1, above. The MIL does not use these technologies in ways that raise privacy concerns other than those discussed in this document. In addition, information that is collected and stored in the MIL (excluding staff usage of the mobile devices) is not combined, loaded to a single database, or otherwise retained or used for purposes other than use in the particular FTC matter in which it was collected. Staff usage of mobile devices is combined with staff access reports and logs to allow the auditing of staff activities to be conducted by DPI and OIG if appropriate.

.7 What law or regulation permits the collection of this information?

Information is collected in the MIL pursuant to the FTC's general law enforcement and investigatory authority, which is primarily set forth in the

Federal Trade Commission Act, 15 U.S.C. §§ 41-58. Other statutes include the Children's Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501; the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act), 15 U.S.C §§ 7701-7713; the Identity Theft Assumption and Deterrence Act of 1998, 18 U.S.C. § 1028 note; the Unlawful Internet Gambling Enforcement Act, 31 U.S.C. 5361 et seq.; the Truth in Lending Act (TILA), 15 U.S.C. §§ 1601-1667f; the Fair Credit Reporting Act (FCRA), 15 U.S.C. §§ 1681-1681(u); the Fair Debt Collection Practices Act (FDCPA), 15 U.S.C. §§ 1692-1692o; the Telemarketing and Consumer Fraud and Abuse Prevention Act (TCFAPA), 15 U.S.C. §§ 6101-6108; the Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801-6809 and §§ 6821-6827; and the Fair and Accurate Credit Transactions Act of 2003 (FACTA), 15 U.S.C. §§ 1681-1681x.

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

As previously discussed, the MIL is used to collect information that is already available to members of the public on the Internet or in the mobile marketplace, or from test sites designed to be accessed solely by the FTC to conduct investigatory analytics. The information that the FTC may collect is the same that consumers might collect or retrieve when accessing the Internet or mobile marketplace from their homes, offices, or mobile device. Therefore, any information that is collected in the MIL from third parties is information that is already available, and the overall privacy risk associated with that information is low. However, a breach or other incident involving information collected or maintained by the MIL could potentially reveal the identity of subjects of non-public investigations or other PII (including sensitive PII) that the FTC may have compiled from public Web sites as evidence to support these investigations, such as PII deliberately or accidently posted on sites, and personal user reviews of mobile apps.

The risk of harm in the event of a breach of such information should be significantly lower than the risk of harm associated with information that has not already been made available on the Internet.

Nonetheless, several safeguards have been implemented to mitigate any residual risks that might be present, and to prevent disclosure of any sensitive information that might be collected. MIL access is physically restricted to authorized users. Information gathered in the MIL is either removed for storage in a limited access file or deleted, destroyed, or overwritten as part of regular MIL maintenance procedures. Information that is removed from the MIL (typically, to be included as part of a larger investigation file[2]), is subject to FTC data protection and

[2] For a discussion of the FTC's system for maintaining non-public investigational and other legal records, see the FTC's System of Records Notice (SORN) I-1, which is available at: http://www.ftc.gov/sites/default/files/attachments/privacy-act-systems/i-1.pdf

privacy policies, including those pertaining to the safeguarding of PII, sensitive personally identifiable information, and sensitive health information.

The Mobile/Internet Lab follows applicable Federal Information Security Management Act (FISMA) requirements to ensure that information collected in the MIL is appropriately secured.

The administrative information that is separately collected about MIL user activities does not create significant privacy risks for MIL users. MIL event and device usage logs only contain FTC work-related information, are accessible only to authorized MIL administrators, and are maintained electronically within the MIL's secure facilities unless required for audits, at which time the requested logs are provided to the FTC's Office of Assurance within OCIO. Original keycard access logs for the Headquarters MIL are maintained and secured by the FTC's security unit.[3] Each month MIL staff review the logs. Logs are not stored on the MIL network.

3 Use and Access to Data in the System

.1 Describe how information in the system will or may be used.

Information is collected to support the FTC's law enforcement mission, as discussed in Section 1, above.

Administrative information collected about MIL user activities is used to track MIL usage and to identify potential system misuse.

.2 Which internal entities will have access to the information?

BCP investigators and case teams will have access to the information collected in the MIL, as will other authorized personnel, as discussed in Section 1, above.

Authorized MIL administrators and OCIO staff will have access to the information collected from MIL usage records.

.3 Which external entities will have access to the information?

As discussed in Section 1, above, the MIL may be accessed by authorized FTC contractors and law enforcement partners.[4] The FTC may also share information collected by the MIL with other external entities that do not have direct MIL

[3] A discussion of the security unit's procedures for maintaining and securing keycard and access log information is available in the PIA for the FTC's Personal Identity Verification (PIV) System and the FTC's Access Control System PIA; all FTC PIAs are located here: http://www.ftc.gov/site-information/privacy-policy/privacy-impact-assessments.

[4] See, e.g., 16 CFR § 4.11 (c), (d) and (j) for information regarding FTC rules for sharing information with law enforcement partners.

access, including, for example, courts, opposing counsel, defendants, expert witnesses, or other individuals as otherwise authorized by the law.[5]

Only pre-approved BCP staff have access to check in/out mobile devices for investigative purposes. Devices or the information collected may be shared for evidentiary purposes with external entities as authorized by the law.

4 Notice and Access for Individuals

.1 How will individuals be informed about what information is collected, and how this information is used and disclosed?

The MIL does not solicit information directly from individuals, except in limited undercover situations, and so does not provide notice to individuals about what information is collected or how it is used. The FTC's Privacy Policy, however, provides consumers and other individuals with general information about how the FTC collects, uses, shares, and protects personal information.[6]

MIL users are required to complete a Rules of Behavior (ROB) form before using the facilities. The ROB explains proper MIL operation and expectations and notifies users of the collection and use of information by BCP and OCIO.

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

The MIL does not solicit information directly from individuals and simply collects information available through the Internet. In some undercover situations, as noted in section 5.1, above, information may be sought directly from an individual. If an individual provides information under such circumstances, he or she would be providing it voluntarily and would have the opportunity to decline to provide it.

MIL users do not have the right to decline to provide administrative and usage information.

.3 Do individuals have the right to consent to particular uses of the information? If so, how would an individual exercise this right?

Individuals do not have an opportunity or right to consent to a particular use of the information collected by the FTC, because the MIL collects information from the Internet and mobile devices that is available to members of the public, whether freely or by registration, membership, or purchase.

---

[5] See, e.g., 16 CFR § 4.11. In addition, the FTC also has internal policies regarding the redaction of PII.

[6] The FTC's Privacy Policy is available at: http://www ftc.gov/ftc/privacy.shtm. In addition, the applicable Privacy Act SORN informs the public about the uses and disclosures of information collected by the MIL. See section 9.

MIL users do not have an opportunity to consent to a particular use of the administrative information that is collected.

.4 **What are the procedures that allow individuals to gain access to their own information?**

If the FTC is maintaining records collected by the MIL on an individual, the individual may make a request for access under the Privacy Act. The FTC's Privacy Act rules and procedures for making such requests are published in the Code of Federal Regulations at 16 C.F.R. 4.13. Individual requests must be made in writing and submitted to the FTC's FOIA/Privacy Act Office in the Office of General Counsel (see http://www.ftc.gov/foia/privactabout.shtm for more information). However, because the primary MIL use is for law enforcement, records about certain individuals (e.g., targets and defendants) may be exempt from mandatory access by such individuals. See 16 U.S.C. 4.13(m) (exemptions applicable to certain FTC Privacy Act systems of records).

.5 **Discuss the privacy risks associated with the process of providing individuals access to their own records and how those risks are mitigated.**

No such privacy risks were identified because individuals are not provided access to their own records through the Mobile/Internet Lab. As discussed in Section 5.4, above, access is provided only by written request to the FTC's FOIA/Privacy Act Office in the Office of General Counsel.

5 Web Site Privacy Issues

.1 **Describe any tracking technology used by the Web site and whether the technology is persistent or temporary (e.g., session cookie, persistent cookie, Web beacon). Currently, persistent tracking technology is not approved for use by the FTC (see 5.2).**

The MIL does not host any permanent websites and is not accessible to third parties. However, in connection with particular matters, FTC staff may set up temporary websites within the MIL to research practices that may be under FTC investigation. To the extent that such research might require the collection of information from or about individuals, staff would consult with the Chief Privacy Officer. None of the temporary websites use persistent or temporary tracking technologies that would collect any information from any member of the public.

.2 **If a persistent tracking technology is used, ensure that the proper issues are addressed (issues outlined in the FTC's PIA guide).**

Not applicable. Temporary websites hosted by the MIL do not use tracking technologies.

.3 **If personal information is collected through a Web site, page, or online form accessible through the Internet, is appropriate encryption used? If not, explain.**

Personal information is not collected through websites hosted by the MIL. Websites used for investigative purposes do not support forms, comment notes, contact information, or other means of collecting personal information.

.4 **Explain how the public will be notified of the Privacy Policy.**

Not applicable.

.5 **Considering any Web site or Internet issues, please describe any privacy risks identified and how they have been mitigated.**

No website privacy issues were identified.

.6 **If the Web site will collect personal information from children under 13, or be directed at such children, explain how it will comply with the Children's Online Privacy Protection Act (COPPA).**

Personal information from children is not collected through websites hosted by the MIL.

6 Security of Information in the System

.1 **Are all IT security requirements and procedures required by federal law being followed to ensure that information is appropriately secured?**

The FTC follows all applicable FISMA requirements to ensure that information collected in the MIL is appropriately secured.

.2 **Has a Certification & Accreditation been completed for the system or supporting program?**

The Mobile/Internet Lab Certification & Accreditation was completed in February 2013.

.3 **Has a risk assessment been conducted on the system?**

The Mobile/Internet Lab risk assessment was completed in February 2013.

.4 **Does the project employ technology that may raise privacy concerns? If so, please discuss its implementation.**

The Mobile/Internet Lab does not employ technologies that raise privacy concerns other than those discussed in this document.

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

Mobile/Internet Lab access is based on organization assignment. All BCP staff are granted access to the Lab as part of the FTC employee check-in process. In accordance with MIL procedures, other FTC staff may request access to the Lab by contacting the Division of Planning and Information's (DPI) Assistant Director. All users of the MIL must sign a ROB agreement before they are granted a MIL network account.

Only BCP staff are permitted to check out mobile devices from the MIL, and for official FTC purposes, mobile devices can only be used outside the lab with approval of their supervisor.

.6 **Describe what privacy training is provided to users either generally or specifically relevant to the program or system.**

All FTC employees are required to complete computer security training and privacy awareness training annually. Interactive online training covers topics such as how to properly handle PII and other data, online threats, social engineering, and the physical security of documents.

In addition, MIL users are required to complete a ROB. MIL users review and sign the ROB annually. MIL Staff notify users on an annual basis of the requirement to resign the ROB. Users failing to do so have their accounts disabled. Persons at the FTC with significant security responsibilities are required to undergo additional, specialized training, tailored to their respective responsibilities.

.7 **What auditing measures and technical safeguards are in place to prevent the misuse of data?**

The following auditing, testing, and technical safeguards are in place to prevent misuse of data:

- Access Enforcement — Active monitoring and testing of access privileges is in place.
- Least Privilege — Fewest folder and file access rights are granted for a user to perform his/her function.

- When a user leaves the FTC, changes roles, or otherwise no longer needs MIL access, that user's rights are removed.
- Privacy risks associated with unauthorized disclosure of information are mitigated through implementation of technical controls associated with need-to-know and least privilege, ensuring that users have no more privileges to data than required to complete their official duties.

Additionally, information gathered during investigatory activities within the MIL is not systematically saved or stored within the MIL. Rather, it is either removed / preserved by staff for use in their investigations, or it is deleted, destroyed, or overwritten as part of regular MIL maintenance procedures. Such information may be copied into a limited access folder on the FTC's production network. This network is part of the FTC's Data Center General Support System, which is protected by security controls outlined by the National Institute for Standards and Technology (NIST) Special Publication (SP) 800-53 Rev. 4, *Recommended Security Controls for Federal Information Systems and Organizations.*

.8 State that any questions regarding the security of the system should be directed to the FTC's Chief Information Security Officer.

Any questions regarding the security of the Mobile/Internet Lab will be directed to the FTC's Chief Information Security Officer.

7 Data Retention

.1 For what period of time will data collected by this system be maintained?

As stated previously, information users may obtain from the Internet or mobile marketplace while using the MIL is not systematically saved or stored within the MIL. Rather, it is either removed / preserved by staff for use in their investigations, or it is deleted, destroyed, or overwritten as part of regular MIL maintenance procedures. The content and context of information generated through use of the MIL conforms to the definition of "non-record materials" as identified in 44 U.S.C. § 3301 and 36 C.F.R. § 1222.14. National Archives and Records Administration (NARA) guidance is to destroy or delete non-records when they are no longer needed. MIL content will be reviewed at least monthly and maintained until removed by the MIL users or administrator.

Information in the MIL, including information, if any, that may be incorporated into or otherwise required to be preserved as Federal records, is retained and destroyed in accordance with applicable schedules issued or approved by the National Archives and Records Administration (NARA).

.2 What are the plans for destruction or disposal of the information?

Disposal of all MIL information will be conducted in accordance with FTC policies and procedures and in compliance with Office of Management and Budget (OMB), NARA, and NIST guidelines. For the destruction of removable media and hard drives, the FTC has retained a vendor whose methods meet or exceed applicable standards for media sanitization and destruction.

.3 **Describe any privacy risks identified in the data retention and disposal of the information, and describe how these risks have been mitigated.**

As stated previously, information users may obtain through the Internet while using the MIL is not systematically saved or stored within the MIL. Once removed from the MIL, the information may be used as evidence or as part of an investigation and stored as needed. For personally identifiable information, the FTC has polices for safeguarding PII.

8 Privacy Act

The MIL is not a system of records retrieved by individual name or other personal identifier under the Privacy Act. Rather, as explained earlier, information that is removed from the MIL is normally incorporated into FTC investigatory files. Those investigatory records are part of the Privacy Act system of records designated as FTC-I-1, Nonpublic Investigational and Other Nonpublic Legal Program Records. MIL user logs, which control user access to MIL resources and track MIL user activities, are part of a separate FTC system of records, see VII-3, Computer Systems User Identification and Access Records – FTC. Key access logs, which record the use of FTC key cards when users access physical MIL facilities, are part of another FTC system of records, see II-11 -- Personnel Security, Identity Management, and Access Control Records System -- FTC. The SORNs describing these FTC record systems are posted on the FTC's public web site at http://www.ftc.gov/about-ftc/foia/foia-reading-rooms/privacy-act-systems.

9 Privacy Policy

The collection, use, and disclosure of the information in the MIL have been reviewed to ensure consistency with the privacy policy already posted on the FTC's main web site, see http://www.ftc.gov/ftc/privacy.shtm

10 Approval and Signature Page

Prepared for the Business Owners of the System by:

_____ Date: _____
David M. Torok
Associate Director, BCP
Division of Planning Information

Review:

_____ Date: _____
Alexander C. Tang, Attorney
Office of the General Counsel

_____ Date: _____
Peter B. Miller
Chief Privacy Officer

_____ Date: _____
Jeffrey Smith
Chief Information Security Officer

_____ Date: _____
Jeffrey Nakrin
Director, Records and Filings Office

Approved:

_____ Date: _____
Bajinder Paul
Chief Information Officer