Federal Trade Commission
Privacy Impact Assessment
for the: Internet Lab

January 2011

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 for purchasing decisions, and confidence in the traditional and electronic marketplaces.

BCP's consumer protection-related activities include consumer complaint collection and analysis, individual company and industry-wide investigations, administrative and federal court litigation, rulemaking proceedings, consumer and business education, and the operation of consumer protection programs. Increasingly, these activities require access to information and services available on the Internet/World Wide Web[1] and in the mobile marketplace.

To support BCP's growing need for Internet-related information and services, BCP has created an "Internet Lab" (Lab). The Lab comprises two main lab facilities in Washington, D.C., as well as nine "satellite locations" (one in Washington, D.C. and one in each of the FTC's regional offices), all of which are secured within FTC buildings or offices.

The Lab is managed by BCP's Division of Planning and Information (DPI). Each regional office has a staff member assigned to administer a Digital Subscriber Line (DSL) machine. DPI and the FTC's Office of Information Technology Management (OITM) staff work together to maintain the Lab.

The Lab 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 Lab may also be used by authorized law enforcement partners (e.g. the Department of Justice), and by 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 OITM. In addition, the FTC may retain experts or contractors who may be given access to the Lab. Individuals in these various groups are referred to in this PIA as "users."

1 System Overview

BCP's Internet Lab comprises various customized commercial off-the-shelf (COTS) hardware and software tools and resources. The Lab provides users with secure and anonymous access to content available on the Internet and mobile devices, and to tools to investigate, capture, and preserve that content. The Lab does not solicit information

[1] This document will use the term "Internet" as the generic term for both the "Internet" and "World Wide Web".

directly from consumers, except in limited undercover situations. Rather, the tools in the Lab allow users to preserve content that is already available to the public on the Internet.

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

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

Connections to the Internet and mobile devices are all registered anonymously, and are not traceable to the FTC. This anonymity allows users to perform research and conduct investigations without being detected. In addition, because neither the Lab nor the mobile devices are able to connect to the production (computer) network used by the rest of the agency, they can be used to access sites which may contain content restricted by FTC web filters; make use of software or apps[2] not available on FTC hardware; and investigate computer viruses and other forms of malware without risk of contaminating the FTC's production computing resources. In other words, users accessing the Internet from the Lab or mobile devices are able to simulate the day-to-day consumer experience.

The Lab provides users with the hardware and software they need to perform investigations and to capture content available on the Internet and mobile devices, including desktop computers, computer 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. audio/video content, web pages, and entire web sites). The tools available in the Lab also provide users with the ability to analyze Internet protocol and website registration information; viruses, spyware, and other forms of malware; "cookies," beacons," computer registry information, and other forms of web tracking technologies; as well as emerging Internet technologies and threats. The Lab also provides users with tools for creating undercover email addresses and web pages, as well as tools for organizing and presenting the information that is obtained.

Information users may obtain from Internet or mobile device usage is not systematically saved or stored within the Lab. Rather, it is either removed/preserved by users for use in their investigations, or it is destroyed as part of regular Lab maintenance procedures.

---

[2] This document will use the commonly used term "app" to identify application software, also known as an "application" or "app", which is used by many mobile devices to perform singular or multiple related specific tasks.

Administrative information concerning user activities within BCP's Lab is also collected. However, unlike information obtained by users as part of an investigation, this administrative information is 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 Lab is used to collect and preserve information that is available on the Internet and mobile devices. As stated previously, the Lab does not solicit information directly from consumers.

Information that is collected may include content freely available or offered through paid/premium services on the Internet or mobile marketplace. This information may include mobile applications or website content, including personally identifiable information (PII) that may be included on the site, as well as usage data and statistics, IP addresses and domain registration and ownership information. PII collected in the Lab 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 publically available on the Internet or mobile marketplace.

Administrative information about BCP's internal Lab activities, including the user's name, phone number (normally an FTC extension), organization code, time and date of entry and exit, and mobile device usage, are collected 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 (e.g. an investigatory target) or by a third party, is collected directly from the Internet or mobile marketplace, and may include content freely available to consumers or content that is only offered through paid/premium services. The Lab does not solicit information directly from consumers.

Administrative information about BCP's internal Lab activities is collected directly from FTC staff 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 above (see section 1). For example, the Lab 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.

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

.4 How is the information collected?

Information is collected in the Lab with the tools described above (see section 2). Information collection is performed by users, and is not part of an automated collection mechanism.

Lab activity and usage information is collected through system event and device usage logs. In addition, the HQ, NJ Ave, and M Street facilities collect physical access information through keycard logs.

.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 point-in-time it was collected.

Lab administrative information is actively monitored by Lab staff, and is subject to review and audits by Information Technology Management Office's (ITMO) Operations Assurance Branch (OAB).

.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 Lab uses mobile devices, apps, and the access to the mobile marketplace for investigative purposes (see section 1). The use of these devices does not use these technologies in ways that raise privacy concerns not otherwise discussed in this document. In addition, information that is collected and stored in the Lab (excluding staff usage of the mobile devices) is not combined and/or loaded in a single database. The FTC is not engaged in data mining and the data is not used for this purpose.[3]

[3] See the Federal Agency Data Mining Reporting Act of 2007, Pub. L. No. 110-53, 121 Stat. 266, §804(b)(1) for a definition/description of the term "data mining."

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

Information is collected in the Lab 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 Lab is used to collect information that is already publicly available on the Internet or mobile marketplace. The information the FTC may collect is the same that which consumers might collect or retrieve when accessing the Internet or mobile marketplace from their homes, offices, or mobile device. Therefore, the overall privacy risk associated with information that may be collected in the Lab is low. However, a breach or other incident could potentially reveal the identity of subjects of non-public investigations.

It is possible that information contained on the Internet or mobile marketplace that may be captured in the Lab may contain "sensitive" information, including sensitive PII. In most cases, the risk of harm in the event of a breach of such information is significantly lower than the risk of harm associated with information that has not been made available on the Internet.

In addition, 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 captured. Lab access is physically restricted to authorized users located within the FTC. Information gathered in the Lab is either removed or destroyed as part of regular Lab maintenance procedures. Information that is removed from the Lab (typically, to be included as part of a larger investigation file[4]), is subject to FTC data protection and privacy polices, including those pertaining to the safeguarding of sensitive personally identifiable information and sensitive health information.

[4] 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/foia/sysnot/i-1.pdf.

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

The information collected about Lab activities does not raise privacy risks for Lab users. Lab event and device usage logs only contain work-related information and are maintained electronically within the Lab's secure facilities until required for audits, at which time the requested logs are provided to the FTC's ITMO OAB. Original keycard access logs are maintained and secured by the FTC's security unit.[5] Each month Lab staff review the logs. Logs are not stored in the Lab.

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 above (see section 1).

Administrative information collected about lab activities is used by the FTC's ITMO and BCP to track Lab 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 Lab, as will other authorized personnel (see section 1).

DPI Lab administration staff and ITMO OAB staff will have access to the information collected from Lab usage records.

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

As discussed in the introduction (see section 1), the Lab may be accessed by authorized contractors and law enforcement partners.[6] The FTC may also share information collected by the Lab with other external entities that do not have Lab access, including, for example, courts, opposing counsel, defendants, expert witnesses, or other individuals as otherwise authorized by the law.[7]

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.

---

[5] 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, which is available at the following location - http://www.ftc.gov/os/2008/02/hrpd12pia.pdf.

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

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

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 Lab 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 notification about how the FTC collects, uses, shares, and protects personal information.[8]

Lab users are notified of the collection and use of information by BCP and ITMO through postings inside the Lab facilities and on the BCP Intranet site.

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

The Lab does not solicit information directly from individuals, and simply collects information available on 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.

Lab users do not have the right to decline to provide administrative 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 Lab collects that information from the Internet.

Lab 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 Lab on an individual, the ndividual 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

[8] The FTC's Privacy Policy is available at the following URL - 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 Lab. See section 9.

16 C.F.R. 4.13. Privacy Act requests must be made in writing and submitted to the FTC's Office of General Counsel (see http://www.ftc.gov/foia/privactabout.shtm for more information). However, due to the law enforcement nature of the system, records in the system about certain individuals (e.g., 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 privacy risks were identified because individuals are not provided access to their own records through the Internet Lab. As discussed above (see 5.4), access is provided only by written request under the Privacy Act to the FTC's 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 Lab does not host any permanent websites. However, the Lab may host a temporary website as required by an investigation. No temporary website uses persistent or temporary tracking technologies. DPI staff review each temporary website for compliance with privacy requirements.

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

Temporary websites hosted by the Lab 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 Lab. Websites used for investigative purposes do not support forms or other means to collect personal information.

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

Personal information is not collected through websites hosted by the Lab.

.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 is not collected through websites hosted by the Lab.

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 Lab is appropriately secured.

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

The Internet Lab Certification & Accreditation was completed in September 2010.

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

The Internet Lab risk assessment was completed in September 2010.

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

The Internet Lab does not employ technologies that raise privacy concerns not already addressed.

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

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 Lab procedures, other FTC staff may request access to the Lab by contacting the Division of Planning and Information's (DPI) Assistant Director.

Only BCP staff are permitted to check out mobile devices.

.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 sensitive PII and other data, online threats, social engineering, and the physical security of documents.

In addition, BCP staff using Lab mobile devices are required to read and acknowledge a mobile device terms and agreement contract annually.

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 — Appropriate folder and file rights are assigned to users to perform his/her function.
>
> 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 Lab, is not saved on any Lab information system. Rather, this information is copied on to the FTC's Infrastructure 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. 3, *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 Lab will be directed to the FTC's Chief Information Security Officer, Margaret Mech, at (202) 326-2609.

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 Lab is not systematically saved or stored within the Lab. Rather, it is either removed / preserved by staff for use in their investigations, or it is destroyed as part of regular Lab maintenance procedures. The content and context of information generated through use of the Lab conforms to the definition of "nonrecord materials" as identified in 44 U.S.C. § 3301 and 36 C.F.R. § 1220.14. National Archives and Records Administration (NARA) guidance is to destroy or delete nonrecords when they are no longer needed. Lab content will be reviewed at least monthly and maintained until removed by the Lab users or administrator.

Once removed from the Lab, information incorporated into FTC records is maintained in accordance with applicable schedules and procedures issued or approved by the National Archives and Records Administration (NARA).[9]

Information collected for the purpose of monitoring Lab usage, including access, system event, and device usage logs, is to be deleted or destroyed when the FTC determines it is no longer needed for audit purposes. The FTC has submitted to NARA a comprehensive records disposition schedule, SF-115 Request for Disposition Authority, Pending NARA approval, FTC will manage usage information in a manner consistent with 44 U.S.C. Ch. 31, 44 U.S.C. 3506, 36 C.F.R. Ch. XII, Subchapter B, Records Management, and OMB Circular A-130, par. 8a1(j) and (k) and 8a4.

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

Disposal of all FTC information collected by the Lab will be conducted in accordance with Office of Management and Budget (OMB), NIST, and NARA guidelines.

.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 from the Internet while using the Lab is not systematically saved or stored within the Lab. Once removed from the Lab, 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 sensitive personally identifiable information and sensitive health information.

[9] For information about retention and disposal of this information, see SORN I-1, Nonpublic Investigational and Other Legal Records (http://www.ftc.gov/foia/sysnot/i-1.pdf).

8 Privacy Act

The Lab itself does not maintain 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 Lab 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. That system is described in a SORN that has been published in the Federal Register and posted on the FTC's Web site (see http://www.ftc.gov/foia/sysnot/i-1.pdf).

9 Privacy Policy

The collection, use, and disclosure of the information in the Lab 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:

Federal Trade Commission

_____
David Torok
Associate Director, BCP
Division of Planning and Information

Review:

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

_____
Marc Groman
Chief Privacy Officer

_____
Margaret Mech
Chief Information Security Officer

_____
Pat Bak
Chief Information Officer

Approved:

_____
Jeffrey Nakrin
Director, Records and Filing Office