Data Privacy & Integrity Advisory Committee

Public Meeting

Thursday, September 10, 2015

1:00 - 4:00 PM
Web Conference Instructions

Please follow these instructions:

CONFERENCE LINE
- Dial 1-888-606-5931 and enter passcode 7283889.
- Please mute your phone but don’t place it on hold.

QUESTIONS
- Hold questions until the end of each session when the operator will open the line. DPIAC members have priority.

HANDOUTS
- This presentation is also available on our website: www.dhs.gov/privacy. Click on Events, then DPIAC Meeting Information.
Welcome & Privacy Office Updates

• Karen L. Neuman, Chief Privacy Officer
New Privacy Officers

• Jamie Danker, Director, Senior Privacy Officer
  National Protection and Programs Directorate, DHS

• John Connors, Privacy Officer
  U.S. Customs and Border Protection, DHS
Briefing on Privacy Incidents

• Kellie Cosgrove Riley, Senior Director, Privacy Policy and Oversight, DHS

• Jeffrey Eisensmith, Chief Information Security Officer, DHS
Committee Tasking

• Karen L. Neuman, Chief Privacy Officer
BREAK: 2:30 – 2:45
DHS Privacy Office
Mobile Applications Policy

• Kellie Cosgrove Riley, Senior Director, Privacy Policy and Oversight, DHS
• David Lindner, Privacy Analyst, DHS
• Rob Palmer, Deputy Executive Director (Acting), Enterprise System Development Office (ESDO), DHS
• Douglas Hansen, Director (Acting), Cloud Enterprise Services, ESDO, DHS
• Christopher Drew, Project Manager, Public Cloud, ESDO, DHS
DHS Privacy Office
Mobile Applications Policy

Background

• DHS Mobile Apps
• Privacy Concerns
• Privacy Policy--DHS Management Instruction
Developing the Policy

- Conducted a comprehensive review of Component’s existing mobile apps and compliance documentation to identify current state of DHS mobile app privacy practices;
- Researched industry and government mobile app privacy practices to identify potential mobile app policy requirements for DHS;
- Worked with OCIO Carwash team to integrate mobile app privacy requirements; and
- Consulted with Components for their feedback on our draft Privacy Policy.
DHS Management Instruction

• The “Privacy Policy for DHS Mobile Applications” is going through formal review as a DHS Management Instruction. Once published, this Instruction will implement DHS Directive 047-01 “Privacy Policy and Compliance” for DHS mobile apps intended for use by the public and/or by DHS employees.

• The Privacy Policy applies throughout DHS regarding mobile apps that are developed by, on behalf of, or in coordination with the Department.
Minimum Privacy Requirements

1. Provide Notice
   - App-Specific Privacy Policy
   - Privacy Statement
   - Contextual Notice
     - Provided upon each update to the mobile app to specifically identify any changes to the uses of information from previous versions of the app;
     - Provided as “just-in-time” disclosures and obtain users’ affirmative express consent before a DHS app accesses sensitive content for the first time (e.g., location services); and
     - Provided with independent opt-out features so that users may customize the mobile app’s features (e.g., opting out of location based services, while still choosing to utilize other app services), where appropriate.
Minimum Privacy Requirements

2. Limit the Collection and/or Use of Sensitive Content

• DHS mobile app features cannot collect and/or use PII, SPII, or other sensitive content unless directly needed to achieve a DHS mission purpose.

• If the collection and/or use of PII, SPII, or sensitive content is directly necessary to achieve a DHS mission purpose, then the collection and/or use of the information must be documented and justified in the PTA.
Minimum Privacy Requirements

3. Establish Guidelines for User Submitted Information
   • Where feasible, use forms and check boxes to limit data collection and minimize data entry errors.
   • Provide a “review before sending” function that allows users to correct or opt-out of sending information to DHS.
   • Unless necessary to achieve a mission purpose, limit ability of users to post information within the app that other users may view.
     – This will limit the potential for sharing PII, SPII, or other sensitive content unnecessarily.
Minimum Privacy Requirements

4. Ensure Mobile App Security and Privacy

- Engage with DHS Carwash to ensure app security and privacy.
- Information submitted through app should be immediately transferred to a protected internal DHS system.
- Sensitive content that a DHS mobile app accesses or uses for the benefit of the user, but that DHS does not need to collect (e.g., location information), should be locally stored within the mobile app or mobile device. This info should not be transmitted or shared with DHS.
DHS Privacy Office
Mobile Applications Policy

DHS Mobile App Development

1. Program Managers and System Managers must notify their Component Privacy Officers or Privacy Points of Contact (PPOCs) and the OCIO Carwash Team before engaging in the development of a DHS mobile app.

2. Component Privacy Officers or PPOCs must engage with the Program Managers and System Managers to ensure the privacy protections outlined in the “Privacy Policy for DHS Mobile Applications” are integrated into the development of the mobile app.

3. Before deployment, the DHS mobile app must go through the DHS Carwash.
DHS Mobile App Development

4. OCIO Carwash team will provide the results of the DHS Car Wash to the Program Managers and System Managers.

5. Before deployment, Program Managers and System Managers, in consultation with Component Privacy Officers or PPOCs, complete a PTA. Component Privacy Officers will compare this PTA to the DHS Carwash results to ensure the PTA accurately describes the DHS mobile app.

6. PTA and results of the DHS Carwash are submitted to the Chief Privacy Officer for review to determine whether the DHS mobile app contains appropriate privacy protections and whether additional documentation is necessary.
DHS Privacy Office
Mobile Applications Policy

DHS Mobile App Development

7. Once it is determined that all necessary Privacy Compliance Documentation is complete, the Chief Privacy Officer will provide final approval for release of the DHS mobile app.

8. DHS mobile apps must go through the DHS Carwash every six months. Existing DHS mobile apps, developed before the implementation of this policy, must go through the DHS Carwash within 6 months of the policy’s issue date.
Carwash strives to provide answers to relevant questions such as:

- What permissions and functionality are used?
- Are users alerted when/if the application performs actions?
- Is data managed securely in storage and in transit?
Carwash – Service Overview

ENVIRONMENT
- A testing, source code management, and requirement/issue tracking environment for building applications
- A centralized service for development teams across DHS

TOOLS
- Open Source Scanning Tools
- Government off-the-shelf (GOTS) Scanning Tools
- Commercial off-the-shelf (COTS) Scanning Tools
- Application Lifecycle Management Tools

REPORTS AND ANALYSIS
- Raw results are provided to tenants automatically after a scan is performed
- The Carwash team provides a summary of results for development teams
Carwash – Mobile App Scanning Process

1. Engage Platform

   - Prepare application binary file
   - Build app externally

   The Developer determines they're ready to engage the DHS/OCIO platform and submits their code and/or binary.

2. Start Cycle

   - Start Cycle
   - Build app externally

   The orchestrator moves source code and binary through each phase of the cycle. If needed, Carwash builds binary from source code. Each cycle outputs a results dashboard.

3. Review Results

   - Review Results
   - Publish App

   The Developer reviews the results dashboard to see how the source code scored against security and privacy measures.

4. Choose Action

   - Choose Action
   - Restart Cycle

   The Developer and program office choose to either make changes to the source code based on the results and restart the cycle, or publish their app.

The Carwash
Carwash – Summary

Results
- Tenants view in-depth reports generated by each of the scanners
- The tools evaluate the mobile app in a number of ways, and scan results may include security, quality, and privacy information
- The Carwash team provides a summary of major findings
- The Carwash team offers a meeting to go through results with the developer and program office

Privacy Interaction
- Privacy team evaluates privacy submission (PTA) and cross references Carwash results to ensure that the intent of the app aligns with what the app is actually doing

Carwash Improvements
- The Carwash Team is constantly evaluating new tools that will help meet security/policy standards
Protecting Privacy in Algorithmic Analytics Programs

Briefing for the DHS Data Privacy and Integrity Advisory Committee

Dan Chenok
Chair, DPIAC Cyber Subcommittee
September 10, 2015
BACKGROUND

• “Behavioral Analytics” – real-time analysis of traffic, seeking to identify anomalies that could point to malicious activity

• NPPD has two pilots underway to develop techniques and assess effectiveness

• Privacy Office and NPPD worked together on potential privacy issues raised by these pilot programs

• Chief Privacy Officer requested that the DPIAC, through the Cyber Subcommittee, make recommendations on how best to protect privacy in such programs

• Cyber Subcommittee met with NPPD and CPO staff for information briefings, in process of developing recommendations for future DPIAC presentation and release
APPROACH

- Define scope of inquiry
- Address key considerations affecting program
- Identify Potential Privacy Protections at each program stage
- Build on related findings from prior DPIAC reports
SCOPE OF INQUIRY

• “Behavioral Analytics” as a term? Subcommittee concerned that this implied tracking individuals

• DHS briefings and discussions led to adoption of alternate term: “Algorithmic Analytics”
  • Descriptive of actual activity: empirical analysis of network traffic activity, collected using automated means, seeking to identify anomalies that could point to malicious activity
    • Establish baselines for patterns of traffic, use machine algorithms to spot anomalous patterns from common baseline
    • Ability to determine potential malicious traffic without knowing a predetermined signature
    • Analyst then does further review to determine if anomaly is associated with a potential problem event (e.g., vulnerability, threat, or incident)
  • Is not signature-based assessment of specific computer-device or application traffic, or assessment of human behavior
SCOPE OF INQUIRY

• Commercial companies engage in AA today -- technologies used include:
  • Front-end authentication
  • Transaction/system monitoring
  • Egress tracking
  • Partnering via multiple accounts
  • Correlation methodologies and tools
  • Analytics and response rules based on empirical scoring
    • Establish baselines for patterns of traffic, use machine algorithms to spot anomalous patterns
    • Determine potential malicious traffic without knowing a predetermined signature
    • Assess if anomaly is associated with a problem event

• Mobile devices present special issues
KEY CONSIDERATIONS

• How is PII affected by AA?
  • Likely to be minimal, situations include:
    • If AA points to individual accounts, could be mishandled
    • AA data could be correlated with PII during analysis phase
    • FIPs come into play
  • When PII involved, rely on existing policies for protection

• Data Quality and Integrity key throughout
  • Includes content of information as well as metadata
  • Focus on integrity of data throughout its use, since AA data itself can be a target
  • Address data governance, including records management

• Accountability
  • Human oversight is vital – allow ongoing reviews, redress
  • Focus on sound procedures, appropriate design, fairness in selecting targets, treatment of PII
  • Privacy Office review of process
POTENTIAL PRIVACY PROTECTIONS AT EACH STAGE

• Collection
  • Develop criteria for what to collect
  • “Strip and Encrypt”, de-identify (where feasible)
  • Provide notice

• Use
  • Define multiple uses—network protection, fraud, website management, etc.
  • Establish process for each use (primary or secondary), use limitations
  • Protocols for follow-up analysis

• Sharing
  • How interface with sharing centers (CERT, NCCIC, etc)?
  • Technical sharing parameters need further focus
  • Define rules for sharing with law enforcement, private sector, ISACs/ISAOs, etc.
POTENTIAL PRIVACY PROTECTIONS AT EACH STAGE

• Access
  • Limit personnel who can work with data
  • Determine rules for when to access
  • Develop controls for access, including logs

• Retention and Disposition
  • Consider how long to retain
    • Limit to shortest time needed for program purpose
    • Caution in establishing fixed time frames – need flexibility as technology and uses evolve
  • Separate AA data from analytics on that data – may need different time frames
  • Establish disposition protocols – how ensure all copies and versions are addressed?
  • Need for security throughout lifecycle and to disposition, consistent with government rules
  • Consider audits, periodic reviews
PUBLIC COMMENTS:
3:45 – 4:00