



Privacy Impact Assessment
for the

Experimental Testing of Project Hostile Intent Technology

February 25, 2008

Contact Point

Larry E. Willis
Human Factors Division
Science & Technology Directorate
(202) 254-6143

Reviewing Official

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780



Abstract

Project Hostile Intent (PHI) is a research effort by the Science and Technology Directorate to ascertain whether screening technology can aid DHS screeners in making better decisions by supplementing the current screening process (wherein a human screener evaluates an individual's behavior) with training and computers. This Privacy Impact Assessment (PIA) addresses privacy impacts of this program, and specifically, the temporary storage of video images during field tests of PHI's performance with real behavioral data to ensure that it is effective in a "real world" environment.

Overview

Project Hostile Intent (PHI) is an experimental research and development (R&D) effort in the DHS Science and Technology (S&T) Directorate. S&T will be the DHS "owner" of the PHI technology while the technology is being developed and refined during the R&D process. S&T will not use the PHI technology to make or support operational decisions. If and when the PHI technology is ready for deployment in an operational environment, a DHS customer (such as the Transportation Security Administration, Immigration and Customs Enforcement, or Customs and Border Protection) will become the "owner" of the PHI technology. Upon operational deployment, the DHS Privacy Office will conduct additional impact assessments.

Laboratory and social science research have associated certain behavioral indicators with deception and/or hostile intent. PHI will use computers to identify and analyze those behavioral indicators, and researchers will assess the ability of the PHI technology to identify those indicators in a real-world setting (such as passenger screening for mass transit) where other factors such as environment (e.g. being too hot) or external stress (e.g., running late for a flight) could produce similar indicators. The specific purposes of this stage of the research are 1) To assess PHI's ability to identify behavioral indicators associated with deception in a real-world environment; and 2) To identify any variations between the indicators produced in the lab and the indicators observed in the field.

Because PHI may ultimately be used by law enforcement customers, the specific behavioral indicators being measured are sensitive information and therefore are not to be discussed in this public document. The goal of PHI is to improve the existing processes by providing screeners with a technology that will help them make faster and better decisions about how to interpret an individual's behavioral responses when answering the screener's questions.

The PHI system will be tested in environments in which an individual is already undergoing screening and thus is already being interviewed by a professionally-trained, experienced screener. Screening could include secondary screening at TSA, but PHI will not be adding any additional screening to existing practices. S&T plans to conduct field testing in the screening environments of several S&T customers. The first planned field test will be with TSA in an airport. The PHI technology will be set up in one secondary screening portal. All persons undergoing secondary screening in the portal where PHI is set up will be videoed. The PHI technology deployed for the field test will not have a video monitor, therefore there will be no inadvertent exposure of the video to anyone in the area. The technology will also not provide any indications or information whatsoever to the screener during the field test. DHS will post notice that video surveillance is occurring. Subsequent field tests with ICE and CBP may involve different



placements of the PHI technology. Regardless of the placement, the PHI technology will be staged such that no feedback provided to the screener by the PHI technology. S&T will take no action whatsoever based on anything observed on the video—these field tests are for R&D purposes only and notice of video surveillance will be placed near the testing environment.

The PHI system will consist of a video camera (without sound recording capability), a computer (to identify specific indicators of deception), and an indicator for the screener (to silently convey the computer's assessment of the individual's behavior). (Note: The indicator will be disabled during field testing such that the screener will receive no feedback from the PHI technology.) The video camera will record an individual's behavior, the computer will analyze the behavior and identify indicators of deception, and the indicator will—when operationally deployed—silently alert the screener, prompting him or her to ask additional questions. The behavioral indicators of deception identified by the PHI system during field testing will later be incorporated into existing training processes and procedures for assessing risk. The addition of the PHI technology when deployed operationally will not change the process that screeners use now (the observation and evaluation of behavior) – the only difference will be that the PHI technology will give the screener more information in determining when to ask additional questions.

For the purposes of the S&T R&D effort, video recordings (without sound) of screening interviews will be retained for further analysis and evaluation of the effectiveness of the PHI technology. The data collected during the PHI experiment will also be used to improve screener training technology. No additional identifying information (i.e. name) will be collected, and the images will not be used by any other component of DHS or by S&T outside the specific PHI effort. The images will be safeguarded through computer security (only authorized personnel will have access to the systems that contain the images) and physical security (the data will be stored and processed at a secure site), and no operational decisions will be made using PHI technology.

Given this project is still in the R&D stage, operational issues have not been addressed, for example how redress will be handled for individuals and what is the best policy for retaining the operational data. These issues will be addressed, prior to any R&D project becoming operational.

Under Subchapter 3 §182 of the Homeland Security Act, the Science & Technology Directorate is charged with “conducting basic and applied research, development, demonstration, testing, and evaluation activities that are relevant to any or all elements of the Department.” This research is being conducted in accordance with that mission to support screening activities conducted by DHS Components such as TSA, CBP, and ICE.

Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed.



1.1 What information is collected, used, disseminated, or maintained in the system?

PHI will collect and use video recordings (without sound) of the behavioral reactions of individuals as they respond to questions posed by the screeners. These recordings are the only personally identifiable information collected or used by PHI. No additional information will be collected (such as the name or any other identifying information related to the passenger), and the data will not be shared with anyone outside the PHI research team.

1.2 What are the sources of the information in the system?

The information will be generated from direct behavioral observation during existing DHS screening processes.

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

The information is being collected and used to test PHI's performance with real behavioral data to ensure that it is effective in a "real world" environment. The technology has already been validated in a laboratory setting, but experiments are necessary to determine if the technology is effective in the environment in which it will ultimately be deployed.

In 2006 and 2007, the State University of New York at Buffalo conducted laboratory testing of the technology. The research was conducted in full compliance with 45 CFR 46, and advance informed consent was obtained from all subjects. In accordance with federal law, the research was reviewed and approved by SUNY Buffalo Institutional Review Board #15 – Social & Behavioral Science. DHS/S&T did not have access to any data collected during the experiment. DHS/S&T received a summary report describing the accuracy of the algorithms being tested.

1.4 How is the information collected?

The video images are collected using a video camera.

1.5 How will the information be checked for accuracy?

The video recordings are being used to test the applicability of technology developed in the laboratory to a real world environment. The information created from direct observation of the individual and is not altered in any way during the research process. The experiment is testing the accuracy of PHI's sensors and algorithms in interpreting behavioral indicators.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

The Homeland Security Act of 2002 [Public Law 1007-296, §302(4)] authorizes the Science and Technology Directorate to conduct "basic and applied research, development, demonstration, testing, and evaluation activities that are relevant to any or all elements of the Department, through both intramural and



extramural programs." In exercising its responsibility under the Homeland Security Act, S&T is authorized to collect information, as appropriate, to support R&D related to improving the security of the homeland.

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

Video recordings, without sound, of screening interviews conducted in a DHS screening environment will be collected and analyzed. The privacy risks associated with this effort exist only because the on-site interviewer knows the identity of the individual at the time of the interview. However, PHI will not have access to names or other identifying data other than the video recordings and no record of the identity of the individual will be created or sought as part of the PHI effort. As an additional safeguard during testing, the PHI collection system used in field testing will not include the use of processing algorithms onsite and will not have video display capability, thus ensuring that no information, outcomes, or results can be transferred from the PHI research to the operational environment.

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

Previous research has identified certain behaviors as being statistically indicative of deception. The information collected will be used to test PHI's performance with real behavioral data to ensure that it is effective in a "real world" environment. The information may also be used to improve screener training technology.

2.2 What types of tools are used to analyze data and what type of data may be produced?

For this testing period, the computer algorithms will be used to analyze the video images after completion of the videotaping back in the laboratory. The data produced by the algorithms will be an analysis of the individual's behavior based on the situation and environment. Statistical analysis techniques will be used to compare the effectiveness of the computer system to the effectiveness of manual analysis of behavior during screening and against the operational outcome of screening interviews (i.e. did the system accurately identify behaviors that correlate with deception/hostile intent?). When operationally deployed, the information from the computer system will only be used to enable the screener to better determine when to ask additional questions. Asking more questions will enable the screener to determine if an individual's behavior is related to deception or a local environmental variable. During the PHI experiment, screeners will not see or use any output of the PHI system during the actual interview process. No operational decisions will be made using PHI technology. The ultimate goal of the PHI system, when operationally deployed, will be to focus screening on individuals who the PHI system indicate are



exhibiting behaviors that suggest deception and further minimize the screening process for other individuals.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

The system does not use commercial or publicly-available data. The only data used in the PHI effort is direct video recordings (without sound) of individuals.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

Information collected through the PHI effort will only be used by the PHI research team within DHS S&T. The data will not be linked to any other identifying information (i.e. name) and the experimental data will be safeguarded through computer security (only authorized personnel will have access to the systems that contain the images) and physical security (the data will be stored at a secure site).

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

The video images and effectiveness ratings will be retained. No Personally Identifiable Information (PII) other than the images will be collected or retained.

3.2 How long is information retained?

The information for this experiment will be retained for the course of the research project and destroyed after that.

3.3 Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?

Yes. General Records System 20 covers the disposition of electronic files or records created solely to test system performance, as well as hard-copy printouts and related documentation for the electronic files/records. Records will be deleted/destroyed when the information is no longer needed.



3.4 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

Risks associated with the storage of personally identifiable information (video recordings) in the experimental system are mitigated by the process by which PHI will safeguard the information: (1) at the experimental site, where the information will be stored on a password-protected, guarded computer and (2) during analysis, where the information will be stored at a secure facility on password-protected systems with restricted physical access. The data will be destroyed when it is no longer necessary for analysis or technical development.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the Department of Homeland Security.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

The PII will not be shared outside of the PHI research team.

4.2 How is the information transmitted or disclosed?

The PII will not be transmitted or disclosed to anyone outside the PHI research team. Any data transfer within the team will occur at a secure site using physical transfer at a secure site (i.e. PHI information will never be exchanged over the internet).

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

The PII will not be shared with or transmitted/disclosed to anyone outside the PHI research team. Any data sharing within the research team will be done using physical transfer at a secure site.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DHS which includes Federal, state and local government, and the private sector.



5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

PII will not be shared outside DHS. Aggregated results (i.e. "PHI is accurate in detecting deception X% of the time") may be shared with potential DHS customers to inform them of the effectiveness of the system.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.

PII will not be shared outside DHS.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

PII will not be shared outside DHS.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

PII will not be shared with or transmitted/disclosed to anyone outside DHS. Therefore, there are no privacy risks associated with external information sharing.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information?

S&T will post signs in the area where the experiment is being conducted. The sign will state: "This area is under video surveillance." Therefore, individuals will be aware that video images are being collected. However, providing explicit notice that to individuals that they are being recorded as part of a screening experiment might alter behavior and would invalidate the results of the research.



The screening environments may also have additional signage posted to notify individuals that an experimental technology is being tested.

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

No. Individuals' behavior is already being observed and evaluated and no operational decisions will be made using PHI technology.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

No, but the information will be used only to evaluate the effectiveness of PHI technology in a "real-world" environment and improve screener training.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

Notice of video recording will be provided to individuals. However, there is still a privacy risk associated with the collection. This risk is mitigated by the fact that the data collected (video recordings) is not linked to any personal identifier and will only be used to evaluate the effectiveness of the PHI technology and improve screener training. The data will also be protected by the computer and physical security measures described previously and no operational decisions will use information from the experimental system.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

7.1 What are the procedures that allow individuals to gain access to their information?

There are no procedures that allow individuals to gain access to their information. The only PII used in this experiment is video recordings, and they will not be linked to any other identifying data such as a person's name. Data collected by PHI will not be accessible to anyone outside the PHI research team and will only be used to evaluate the effectiveness of the PHI technology and improve screener training technology.



7.2 What are the procedures for correcting inaccurate or erroneous information?

The information is created from direct observation of the individual and is not altered in any way during the research process. The experiment is testing the accuracy of PHI's sensors and algorithms in identifying the behavioral indicators of deception.

7.3 How are individuals notified of the procedures for correcting their information?

As the video recordings are collected through direct observation and are not linked to an individual, there are no procedures for correcting inaccurate or erroneous information.

7.4 If no formal redress is provided, what alternatives are available to the individual?

There are no alternatives available to the individual. This is a research effort and the recorded PII is not used to make decisions or determinations that impact the individual recorded. If and when PHI is deployed operationally, the DHS Privacy Office will re-assess the privacy impacts associated with the project.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

The information collected consists solely of video recordings that are not linked to any other personal identifier. The information is collected by direct observation of actions. The privacy risk is mitigated by the fact that the information will be protected by computer and physical security procedures and will only be used to evaluate the effectiveness of the PHI technology and improve screener training technology.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

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

During experimentation, only pre-selected and trained screening personnel will have access to the video images and effectiveness ratings. For analysis, only PHI team members will have access to the information. The information will be accessed and used only to analyze the effectiveness of the PHI technology and improve screener training technology.



8.2 Will Department contractors have access to the system?

Yes; only PHI research team contractors will have access to the system.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

Each operator, maintainer, and PHI team member will receive a review of the security features of the demonstration prototype and will be trained on DHS privacy policies.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

Due to the architecture and existing security precautions of PHI, a full Certification and Accreditation (C&A) is not required, as acknowledged by the DHS Office of the Chief Information Officer.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

The systems on which the information is stored are protected by role-based password access and physical security. The systems on which the information is stored will connect only to authorized government networks, as specified in the C&A documentation.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

Only authorized users can access the information, which is protected by firewalls, password security, and physical security. Therefore, the privacy risks associated with technical access and security have been mitigated.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1 What type of project is the program or system?

PHI is a research and development project in DHS S&T.



9.2 What stage of development is the system in and what project development lifecycle was used?

PHI is not yet a system and is in the validation and verification phase of R&D. The technology has already been validated in a laboratory setting, but experiments are necessary to determine if the technology is effective in the environment in which it will ultimately be deployed.

As of yet, the PHI research team has not used a life cycle planning tool.

9.3 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

This experiment collects video recordings of interactions that are already being observed by DHS screeners in the existing procedures. These recordings will not be linked to any other personal identifier and will not be shared with anyone outside the PHI research team. The information will be collected and maintained only long enough to validate the effectiveness of the technology. The aggregated information regarding behavior indicators will be used to improve screener training technology.

Approval Signature Page

Original signed and on file with the DHS Privacy Office

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security