Privacy Impact Assessment
for the

Cell All Demonstration

March 2, 2011

Contact Point
Stephen Dennis
HSARPA Technical Director
(202) 254-5788

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The Cell All project is a research, development, testing and evaluation effort funded by the Homeland Security Advanced Research Projects Agency (HSARPA) in the Department of Homeland Security Science and Technology Directorate (DHS S&T). Cell All is an environmental surveillance system that uses a typical cell phone as a platform for a sensor system to detect harmful chemical substances and transmit critical information, including location data, to first responder and other related monitoring agencies. With the sensors suite developed and fitted on a cell phone, S&T will conduct a demonstration of the prototype system using research-owned devices. While no personally identifiable information will be collected during the demonstration, S&T is conducting a PIA to address the privacy impact of the transmission of location data using the prototype.

Introduction

S&T has awarded contracts to three research performers, the National Aeronautics and Space Administration (NASA), Qualcomm, and Synkera Technologies Inc., through HSARPA and the Small Business Innovation Research portfolio to provide funding for the research, development, testing and evaluation (RDT&E) of the Cell All system and network. Conceptually, the Cell All system is a personal environmental threat detector system, consisting of multiple sensors which are miniaturized into a device and applied on an individual's cell phone. Cell All uses an individual's cell phone as its platform for sensors to detect harmful substances in support of first responder operations. The Cell All system will integrate sensors into cell phones to allow its users to continually test the surrounding environment for harmful substances and send alerts to a central monitoring agency (e.g., first responders) if it detects an exposure or abnormal quantities. Cell All also integrates the Global Positioning System (GPS) function found on typical cell phones.

It is envisioned that in the event Cell All detects the presence of an abnormal chemical substance or large quantities of a chemical substance (e.g., carbon monoxide, ethanol, chlorine, hydrogen cyanide, and toluene), the system will transmit the time and place (latitude and longitude coordinates) of the specific event to a monitoring agency through the Cell All network. Using this information, first responders will be able to analyze the situation and verify whether it is a real emergency or a false alarm, and respond accordingly, facilitating the appropriate resource and/or personnel distribution. For example, if first responders receive one alert of toluene (paint thinner) presence, and find that the individual is at a construction site, they may determine it is a false alarm or not an emergency situation. However, if they receive multiple detections of a poisonous gas in a public park, they may respond to it as a potential bioterrorist attack. Ideally, the system would alert first responders of the type of chemical emergency, the number of alerts or exposures, and the exact location of the incident, which would enable emergency operation centers to determine which area hospital would require the most staff and equipment and ensure that appropriate treatment is available.

The Cell All project is a multi-phased RDT&E project that began as a proof of concept (phase I). Phase I of the program consisted of the research and development of a suite of chemical sensors (e.g., carbon monoxide, ethanol, chlorine, and toluene). In phase I of the project, research performers also developed the GPS/location function to ensure accurate location information and chemical readings.

The Cell All program is now beginning phase II and will test and demonstrate the prototype system at the Los Angeles Fire Department test facilities. The test facilities provide a simulated test environment that is similar to real life settings (i.e., hotel rooms, buildings, etc.). Individuals from the first responder community, stakeholders, and S&T program managers are going to be present during the demonstration. All participation in the demonstration is voluntary. The cell phones' platform used in the prototype are DHS- or researcher-owned devices; no members of the public are impacted by this demonstration. The objectives of the demonstration are to: (1) determine the viability, accuracy, and effectiveness of the chemical sensors; (2) determine whether the GPS function can accurately track location information and correlate it with the sensor readings; and (in some cases) (3) examine how effectively the prototype transmits information to the test network.

The demonstration is comprised of various scenarios; all scenarios are conducted in a test setting, using a stand alone, test network that is not connected to any other systems. The scenarios conducted include:

- Testing of indoor release of gas, likely carbon monoxide, in a hotel-like room. Multiple devices are placed throughout the room to determine whether or not the sensor can detect the presence of the gas.
- Testing of indoor release or spill of a chemical in a simulated chemical facility. Multiple sensors are placed throughout a simulated chemical facility to determine whether or not the sensor can detect the chemical spill.
- Testing the release of gas in an indoor stadium (tentative).
- Testing the release of gas outdoors (tentative),

During the demonstration, chemical readings captured from the simulated scenarios as well as location data are transmitted to the test network. The cell phone number is also transmitted; however this information is scrubbed by the cell phone provider (per agreements with S&T) and is not displayed in the final output. For demonstration purposes, information is not transmitted to first responders or other monitoring agencies. No personally identifiable information (PII) is used, captured, or transmitted during the demonstrations. Once the proof of concept and prototype system is validated, external vendors will be responsible for transitioning and marketing the system; DHS S&T is not responsible for deploying the system. Privacy protection associated with the operational use of the chemical and location data and network security and encryption techniques will be considered and implemented by the end users of the system. Decisions regarding the capture and transmission of additional information (e.g., phone numbers, names of cell phone owner) will also be decided by the end user community, with input from the first responder community, and public health organizations, among others. Once deployed, the end user community will be responsible for conducting periodic audits of the Cell All system. Of particular importance is the assurance that the sensors are only collecting the detection of an abnormal chemical substance and the user's location, and that such data is securely retained.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974 articulates concepts of how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information. The Homeland Security Act of 2002 Section 222(2) states that the Chief Privacy Officer shall assure that information is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974.

In response to this obligation, the DHS Privacy Office developed a set of Fair Information Practice Principles (FIPPs) from the underlying concepts of the Privacy Act to encompass the full breadth and diversity of the information and interactions of DHS. The FIPPs account for the nature and purpose of the information being collected in relation to DHS's mission to preserve, protect, and secure.

DHS conducts Privacy Impact Assessments (PIA) on both programs and information technology systems, pursuant to the E-Government Act of 2002 Section 208 and the Homeland Security Act of 2002 Section 222. This PIA is conducted as it relates to the DHS construct of the Fair Information Principles. This PIA examines the privacy impact of the Cell All Project Demonstration as it relates to the Fair Information Principles.

1. Principle of Transparency

Principle: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII. Technologies or systems using PII must be described in a SORN and PIA, as appropriate. There should be no system the existence of which is a secret.

Cell All is designed as a user-based system. Once deployed, users voluntarily apply the Cell All system to a phone by signing up for the Cell All surveillance system. Information about the Cell All system is provided to the user prior to signing up for the service. By applying the Cell All system to the phone, the user understands that the sensors are working and that location data may be transmitted to a first responder monitoring agency in the event of a chemical detection. Furthermore, the user is notified by the system when his or her location data is released.

Individuals from the first responder community, stakeholders, and S&T program managers are going to be present during the demonstration. All participation in the demonstration is voluntary.

2. Principle of Individual Participation

Principle: DHS should involve the individual in the process of using PII. DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of PII and should provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.

The design of Cell All enables the user to control when to use the system. They are able to turn off the Cell All sensors at anytime, thus enabling them to control when data will be transmitted. Once deployed, users voluntarily sign up for the Cell All system. By applying the Cell All system to the phone, the user understands that system may transmit information to a first responder monitoring agency in the event of a chemical detection.

During the demonstration, individuals from the first responder community, stakeholders, and S&T program managers are going to be present during the demonstration; however, no PII is used, captured, or transmitted during the Cell All demonstration. All participation in the demonstration is voluntary. No members of the public are impacted by the demonstration.

3. Principle of Purpose Specification

Principle: DHS should specifically articulate the authority which permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.

Cell All's purpose is narrow; use a specific sensor to read the environment and determine whether any chemical hazards are present and notify a first responder of its presence and location. However, for the purpose of the demonstration, no data is transmitted to first responders. There is no other use for the sensors or the collection of location data.

During the demonstration, chemical readings from the simulated scenarios along with location data (longitudinal and latitudinal coordinates) are transmitted to a test server. The test server is a standalone system that is not connected with any DHS or first responder system. The data collected during the demonstration is only used for RDT&E purposes, to validate the proof of concept. The data is not used for any other reasons.

4. Principle of Data Minimization

Principle: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA).

Cell All limits the collection of data to only what is relevant and necessary for first responders. Chemical readings and location data are transmitted during the demonstration. The cell phone number is also transmitted; however, per agreement with S&T, the cell phone provider scrubs the phone number during transmission and it is not displayed in the final output. The chemical reading and location data are necessary to determine the effectiveness and utility of the Cell All prototype. No other information is collected or used during the demonstration.

Chemical and location data will be retained after the demonstration to support further research and development efforts; no PII will be retained.

5. Principle of Use Limitation

Principle: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.

Cell All's sensors only collects information regarding a chemical substance detection and the cell phone's location; no other information should be shared.

The data captured during the demonstration is only used for RDT&E purposes. Additionally, no PII is captured, used, or transmitted during the demonstration.

6. Principle of Data Quality and Integrity

Principle: DHS should, to the extent practical, ensure that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.

The Cell All system is undergoing extensive testing to ensure the accuracy of the data transmitted.

The purpose of the demonstration is to validate the proof of concept and determine the effectiveness and utility of the Cell All prototype. Any chemical reading or location data, whether it is correct or incorrect is valuable to the evaluation, analysis, and improvement of the system. No PII is captured, used, or transmitted during the demonstration.

7. Principle of Security

Principle: DHS should protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

Privacy protection associated with the operational use of the chemical and location data and network security and encryption techniques will be considered and implemented by the end users of the system.

During the demonstration, the Cell All prototype captures and transmits the chemical reading and location data. No PII is captured, used, or transmitted during the demonstration; therefore, no additional security safeguards are employed to secure the transmission of this data.

8. Principle of Accountability and Auditing

Principle: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and should audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

All S&T program managers and contractors receive privacy awareness training on an annual basis. The performers do not handle any PII during the demonstration; therefore no privacy training is provided prior to the demonstration.

Conclusion

Once the Cell All system is validated during the demonstration, external vendors will be responsible for transitioning and marketing the system for operational use. DHS S&T is not responsible for deploying the system. Privacy protection associated with the operational use of the chemical and location data and network security and encryption techniques were considered as part of the pilot. Decisions regarding the capture and transmission of additional information (e.g., phone numbers, names of cell phone owner) will also be decided by the end user community, with input from the first responder community, and public health organizations, among others.

The system has been designed to work so that information is not always required thus reducing the impact on privacy. As described above, per agreement with S&T, the cell phone provider scrubs the

phone number during transmission so it is not displayed in the final output. Once deployed, however, the end users and stakeholders will independently determine whether or not cell phone numbers are necessary to conduct an effective emergency response (i.e., contact impacted individuals) or whether it should continued to be scrubbed. The end users will also be responsible for conducting periodic audits of the Cell All system. Of particular importance is the assurance that the sensors are only collecting the detection of an abnormal chemical substance and the user's location, and that such data is securely retained. While Cell All was designed with privacy protections in mind, the end user community must continue to consider privacy when deploying the system for operational use.

Responsible Officials

Stephen Dennis
Program Manager
HSARPA Technical Director
(202) 254-5788

Approval Signature

Original signed and on file with the DHS Privacy Office.

_____

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780