Privacy Impact Assessment
for the

Gaming System Monitoring and Analysis Effort

DHS/S&T/PIA-025

October 11, 2012

Contact Point
Douglas Maughan
DHS S&T Cyber Security Division
202-254-6145

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Gaming System Monitoring and Analysis project is a research effort funded by the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) Cyber Security Division (CSD) to design and develop forensic tools for extracting data from gaming systems. S&T is conducting a Privacy Impact Assessment (PIA) because gaming systems used in this research project may contain personally identifiable information (PII).

Introduction

In 2008, DHS S&T was approached by the law enforcement community for assistance in researching a capability to investigate potential crimes being conducted through the use of modern gaming systems. Today's typical gaming systems have processing, multimedia, and networking capabilities rivaling personal computers. Not only are they used to play video games, wireless capabilities enable users to interact and communicate with other players, browse and purchase items over the internet, and stream videos onto their systems. As a result, these gaming platforms are increasingly being used by criminal pedophiles as a tool for identifying and exploiting children. Because of their use by criminals, some gaming systems are being seized by U.S. law enforcement agencies during court-authorized searches.

The research and analysis of gaming systems is a relatively unexplored area of digital forensics. At the present time the U.S. government and U.S. law enforcement agencies' capabilities to track, engage, and record criminal activity on these systems is limited by a number of factors, including the fact that each gaming system platform uses its own proprietary architecture, software, and communications protocols. The lack of forensic methods for extracting and analyzing information from game consoles is problematic for law enforcement's efforts to investigate and combat criminal activities.

The purpose of this project is to research and examine the types of information that may be present on a gaming console (including chat logs) and accessible by law enforcement during an active criminal investigation.

The Naval Postgraduate School (NPS) was selected by DHS S&T to complete this work because of its related expertise in the area—specifically the development of the Real Data Corpus (RDC) and its experience in developing open source tools for bulk data analysis. DHS S&T is funding this effort to research and develop forensic tools that can support law enforcements efforts to investigate game consoles and similar electronic devices. The forensic tool will be made available by NPS for law enforcement users. S&T will receive a final report from NPS at the end of this project.

The RDC is a set of raw data extracted from hard drives, flash memory cards, cellular telephones, and other data-carrying devices that were purchased on the secondary market outside

the United States. Raw data may include web browsing history, chat logs, email addresses, among other data elements. The RDC is currently housed at NPS. Its use for the development of computer forensic tools has been approved by multiple Institutional Review Boards (IRB). Unlike data that is created in a laboratory environment, the structure and content of data in the RDC is both unpredictable and uncontrollable. The data also have a scale and diversity that approaches the scale and diversity of data recovered during actual law enforcement operations. The RDC is typically used as simulated or test data for developing and testing new computer forensic algorithms. This is vitally important, as forensic tool developers typically cannot obtain access to actual case data due to legal restrictions.

As is NPS practice, NPS restricts its purchasing of used gaming consoles to systems that have been sold or disposed of by their previous owners outside the United States. Previous experience has shown that used equipment purchased inside the U.S. is highly likely to contain U.S. Person[1] data, while equipment purchased outside the U.S. is less likely to contain such data. As a second level of protection, NPS researchers and NPS contractors protect the information using access control technologies and generally do not attempt to identify any individuals whose information may reside inside the data carrying devices. For most of the project, data is used in aggregate form where it is processed and analyzed in bulk. On occasion, forensic tools used against the RDC may have the capability to extract personal data elements. In such cases, researchers take due diligence to examine the data, in accordance to NPS policies and standards, and deduce whether it belongs to U.S persons. If they find the data may belong to U.S. person, the data is removed from the Real Data Corpus. Finally, NPS policy prohibits the use of data in the RDC from being used in actual cases or for training purposes; the use of the data is limited only to research purposes. No individuals (U.S. Persons and non U.S. persons) are impacted if their data is extracted from the gaming consoles during this project.

The RDC and its data are owned and controlled by NPS. DHS S&T is not provided access to the personal information or data on the gaming consoles purchased for this project. Access to that data is limited to NPS researchers and contractors.

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.

[1] U.S. Person refers to United States citizens and lawful permanent residents (LPRs).

In response to this obligation, the DHS Privacy Office developed a set of Fair Information Practice Principles (FIPP) 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 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. Given that the Gaming System Monitoring and Analysis project is a software tool rather than a particular information technology system, this PIA is conducted as it relates to the DHS construct of the Fair Information Principles. This PIA examines the privacy impact of the Gaming Systems Monitoring and Analysis research and development work 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.

The gaming consoles that are purchased for use during this research project are intentionally bought from markets outside of the United States to avoid the collection of PII from U.S. Persons. NPS immediately deletes any U.S. Person's PII extracted from devices that it acquires under this project. DHS S&T is not collecting the information extracted from the consoles used in this effort, nor will the information be used for any law enforcement investigation. The forensic tools developed from this effort will be distributed to the public by NPS as open source software.

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 gaming consoles being purchased for use during this research project have been sold or disposed of by their previous owners. The gaming consoles are intentionally purchased from markets outside of the United States to avoid the collection of PII from U.S. Persons. NPS deletes any U.S. Persons data found on the devices. DHS S&T does not receive any PII from the purchased gaming consoles.

3. Principle of Purpose Specification

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

Law enforcement agencies require forensic tools that can extract information from gaming consoles seized during investigations. DHS S&T is funding this effort to research and develop forensic tools that can support law enforcements' efforts to investigate game consoles and similar electronic devices. DHS S&T will not use any data collected for operational law enforcement purposes.

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).

DHS S&T is not collecting any PII. Any non-U.S. person PII found in the gaming consoles may be included in the RDC, which is used to research, develop, and test prototype systems. The RDC is owned and controlled by NPS; DHS S&T does not receive any PII from the RDC. NPS uses computer security access controls to protect the PII that resides in the RDC If any PII belonging to U.S. persons is identified, NPS immediately removes the data from the RDC.

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.

The non-U.S. Persons information is extracted from the gaming consoles and added to the RDC for the purpose of developing digital forensics tools. This use of the information has been approved by the NPS Institutional Review Board for research. There are no other uses for this information. Any information belonging to U.S. persons is immediately deleted.

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.

During the course of this research project, non-U.S. person PII extracted from the gaming systems purchased will be utilized by the researcher to develop and test new digital forensics tools. There will not be any exchange of information to DHS and the data will only be housed in

the RDC.

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.

DHS S&T does not receive any PII collected during this research project; that information remains in the RDC and controlled by NPS. The deliverables that DHS S&T receive for law enforcement customers will be the forensically-sound data extraction tools that are used for investigative purposes, and as admissible in a court of law.

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 DHS S&T personnel are required to receive privacy awareness training on an annual basis. However, DHS S&T is not receiving or collecting any PII during this research and development project. The PII found on the gaming systems and collected in the RDC during the effort is not U.S. persons data and remains with NPS as part of the RDC.

NPS uses computer security access controls to limit access to the Real Data Corpus and retains a list of all researchers that have had access to the data. All proposed research involving the RDC must first be approved by an Institutional Review Board with a DoD assurance.

Conclusion

The goal of the Gaming System Monitoring and Analysis effort is to research and develop a forensic tool that can extract data from gaming consoles for law enforcement and investigative purposes. During this project, NPS collects gaming consoles that have been sold by their previous owners. NPS only purchases gaming systems from outside the U.S. to minimize PII collected on U.S. Persons. Any non-U.S. Persons PII is retained on the RDC and used to test and validate the developed forensic tool. Any operational use of the tool is outside the scope of this PIA; a separate PIA will need to be conducted by any DHS operational component that plans to deploy the tool for operational use.

Responsible Officials

Douglas Maughan
DHS S&T Cyber Security Division

Approval Signature Page

Original signed and on file with the DHS Privacy Office.

_____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security