Homeland Security Wants Access to Your XBox

According to various reports, the Department of Homeland Security has initiated a program designed to provide the snoops a mechanism for hacking gaming consoles to uncover users' critical personal data.

As one of the first steps toward achieving this nefarious goal, the Department of the Navy was tasked by DHS with awarding a contract to Obscure Technologies to "fund the development and delivery of computer forensic tools for analyzing network traffic and stored data created during the use of video game systems."

The California-based company will receive over $177,000 toward research and development of the tools that will give the federal government the backdoor access to financial and personal data it desires.

The Navy was chosen to oversee this contract "because of the expertise of Simson Garfinkel, a computer science professor at the [Naval Postgraduate School] in Monterrey, California."

What is DHS expecting in return for its investment in Obscure Technologies?

As set forth in the terms of the contract, DHS demands:

> This project proposes to create the following deliverables for use by Department of Homeland Security Science and Technology (DHS S&T):
>
> Hardware and software tools that can be used for extracting data from video game systems.
>
> A collection of data (disk images; flash memory dumps; configuration settings) extracted from new video game systems and used game systems purchased on the secondary market.

In order to conduct the appropriate tests, Homeland Security instructs Obscure Technologies to purchase "video game systems outside the US in a manner that is likely to result in their containing significant and sensitive information from previous users." Not exactly obscure language. DHS is apparently flush with power and has no need to hide its intentions behind vague language.

One of the chief aims of the experiment is described as the extraction of private information that may be included in communication exchanged between users chatting online.

Of course, this project (like so many others) is nothing more or less than a high-tech violation of the Fourth Amendment "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."

Why would Big Brother be interested in monitoring your adventures in online realms? One of our federal overlords' favorite straw men is once again propped up in this struggle to combat the evils of "terrorism."

How do the feds know that terrorists are using gaming consoles to communicate? They don't, but according to John Verrico, spokesman for DHS's Science and Technology Directorate, "there is suspicion" that they are doing so.

In a world where the Constitution is viewed as "flawed" and no more than a passé paper impediment to the implementation of an omnipotent, omniscient central government, mere suspicion on the part of some executive branch apparatchik is enough to justify spending hundreds of thousands of taxpayer dollars on the development of a device to copy critical data from entertainment devices sitting otherwise safely in the homes of law-abiding American citizens.

Foreign Policy discloses that the effort has been underway since 2008 under the project named "Gaming Systems Monitoring and Analysis Project." In an e-mail sent to *Foreign Policy* by the NPS expert mentioned above, we learn that the purpose of the program is to "improve the current state-of-the-art of computer forensics by developing new tools for extracting information from popular game systems, and by building a corpus of data from second-hand game system that can be used to further the development of computer forensic tools."

That description is faithful to the double-speak and vague terms that are the patois of that segment of the federal bureaucracy dedicated to domestic spying.

Evidence suggests that it must not be as easy to hack these game consoles as it would otherwise seem. Three years ago *Science Daily* reported that the government was trying to tap these devices for information.

> A forensics toolkit for the Xbox gaming console is described by US researchers in the International Journal of Electronic Security and Digital Forensics. The toolkit could allow law enforcement agencies to scour the inbuilt hard disk of such devices and find illicit hidden materials easily.

The text of the contract setting out the guidelines of the project indicates that it is precisely this difficulty that prompted DHS to select Obscure Technologies to receive its investment in invasion:

> Analysis of the game systems requires specific knowledge of working with the hardware of embedded systems that have significant anti-tampering technology. Obscure Technologies has substantial experience in working with such systems. Obscure Technologies has the ability to do cradle-to-grave turnkey servicing of complete hardware systems design.

As hard as the hacking might be, researchers at Drexel University insist that they have been able to extract credit card information and a billing address from the hard drive of an XBox 360 even after the user tried to erase it by reformatting the drive.

As a paean to privacy, Garfinkel assures readers that DHS has no intention of using the product provided them by Obscure Technologies on consoles owned by American citizens living in America. Said Garfinkel:

> This project requires the purchasing of used video game systems outside of the U.S. in a manner that is likely to result in their containing significant and sensitive information from previous users. We do not wish to work with data regarding U.S. persons due to Privacy Act considerations. If we find data on U.S. citizens in consoles purchased overseas, we remove the data from our corpus.

In other words, if the government finds any information on a machine they acquire overseas that contains data relevant to American citizens, they will disregard it.

Readers will certainly know that such promises are illusory at best and these assurances will be abandoned in favor of the new list of guidelines handed down recently by Attorney General Eric Holder. According to Holder, those agencies of the federal government tasked with combating "terrorism" may retain data gathered about American citizens indefinitely even if it contains no connection to criminal activity whatsoever. There is no exception made for data obtained overseas.

In fairness, DHS is probably less interested in the credit card numbers of people playing games online than in the content of chat logs kept of conversations carried on by those suspected of using that medium to plan terrorist attacks.

Witness this story published four years ago in *Wired* magazine:

> Having eliminated all terrorism in the real world, the U.S. intelligence community is working to develop software that will detect violent extremists infiltrating World of Warcraft and other massive multiplayer games, according to a data-mining report from the Director of National Intelligence.
>
> The Reynard project will begin by profiling online gaming behavior, then potentially move on to its ultimate goal of "automatically detecting suspicious behavior and actions in the virtual world."

Despite the despicable constitutional deprivation involved in their work for the Department of Homeland Security, Obscure Technologies president Gregory May seems excited by the prospect (and undoubtedly by the $177,000 and change his company pockets from the job). He told *Foreign Policy* magazine that the task is still in the "exploratory research and development" stage. "It will be interesting to see, because it's new to us as well," he said. "A lot of this stuff hasn't been done. We're not sure how complicated it is." Certainly not too complicated to dissuade the feds from following it up, however.

The opposing point of view was provided to *Foreign Policy* by a familiar foil of federal spying schemes, the Electronic Frontier Foundation (EFF). Parker Higgins, a spokesman for EFF, told *Foreign Policy* that he worried that those using these popular game consoles are likely unaware of how much personal data is stored on the hard drives in those machines.

"These consoles are being used as general-purpose computers. And they're used for all kinds of communications. The Xbox has a very active online community where people communicate. It stands to reason that you could get sensitive and private information stored on the console," Higgins said.