I Like Watching You: Playing with Privacy in the Gaming Age

posted by: Aaron Stanton
http://ispots.mit.edu/

keywords: spyware privacy legal culture wifi Sony MIT

With items like Sony’s ever-entertaining rootkit making mainstream news, your personal computer has suddenly become a very public place.

Now, new technology introduced at one of the United States’ most prestigious research universities has the potential to make the privacy concern a matter of physical location instead of intellectual property.

The Massachusetts Institute of Technology’s new wireless Internet system tracks the physical location of its users.

The campus-wide wifi network is able to locate connected computers on a 3D plain, making it capable of distinguishing between computers logging in from different rooms and different floors within one building. Or anywhere on campus.

With user permission, names and locations are then displayed on monitors throughout MIT’s campus. Without venturing outside, students can now check to see how many
laptops are in the campus coffee shop, or locate their wired friends between classes.

Yet in an era plagued with growing concerns of constitutional violations, government people-watching, and behavioral tracking systems, how much do we want our technology to keep tabs on us?

Dr. Carlo Ratti, director of the MIT's SENSEable City Laboratory, understood this concern when the laboratory started work on the project, and helped build the school's new system with privacy issues in mind.

"This map computes the traces of individuals passing through the MIT campus. Users who are mapped have given their agreement and are managing their visibility at their own will."

From iSpots' Project Website

"It is impossible," Dr. Ratti says, referring to worries that an individual's location might be tracked and recorded without the user's permission. "One of our goals is to give people the control of the locational data."

Even if administrators were inclined, or compelled, to share information on a person's movements, Dr. Ratti is quick to point out that such identifying markers aren't available without the say-so of the user.

"(The users) should decide how to manage and share (that data) on a peer-to-peer basis," Dr. Ratti says. "In the next weeks a new applet will give full control on the data to the users. They can decide to opt out whenever they want."

Such comments are reassuring to privacy-conscious members of the public worried that the system might be adapted to keep
an eye on people without their knowledge.

Their concerns are not without justification.

Corporate forays into consumer information gathering have not gone well, of late. Sony's rootkit-based attempts to curb copyright infringement come to mind, a developing fiasco that's left an estimated 500,000 computer networks vulnerable to hacking, and Sony facing lawsuits.

Princeton DRM researcher Ed Felten analyzes Sony's rootkit "remover" and concludes that it's a hunk of junk: "they're almost certainly adding things to the system...they're not disclosing what they're doing."

From Rootkit Timeline on BoingBoing.net

When given the power to watch consumers without permission, corporate and government entities have not always behaved themselves.

As public wifi connections become more common, so too will the possibility for privacy violations.

It's hard to find a coffee shop anymore without some form of wireless Internet access, often needed to serve an increasingly tech savvy consumer. Even McDonald's lets you surf the net and play games online, following a deal with Nintendo to provide free wifi service to Nintendo DS owners. Already, cities like San Francisco and Philadelphia have declared their intention to pursue a variety of municipal broadband projects designed to blanket entire communities with wifi access.

Soon, Internet access will follow you wherever you go.

It's important that institutional limitations be
established during the growth phase of wide-scale public Internet implementation. Already, precedent is being set that allows companies to develop and implement programs such as Sony's rootkit.

In a recent interview, Microsoft's Marketing VP Peter Moore commented that the Xbox 360 might update itself automatically, with the user, "(possibly) not even aware (that it) happens."

Considering the prevalence of online gaming in the console era, these kinds of rights management and anti-piracy/hacking measures may be unavoidable to consumers and tempting to companies. Xbox Live is now included with every Xbox 360 at the free "Silver" level. And Sony has affirmed it's "wild west" style of online gaming, wherein game companies have ultimate freedom to develop applications that could, for example, send information about what other game saves you have on your memory card.

Similar elements exist inside of the Windows operating system. Windows Media 8 was found to record what DVDs are played on your system and transmit that data to Microsoft servers, something not specified in the user agreement at the time. Microsoft's solution to this concern was not to stop tracking the data, but simply to include a mention of the practice in the long legal preamble that appears before you use the software.

There's some question about whether or not it's fair that such established systems operate on a policy of, either "Deal With It, or Move On," with no ability to disable the data gathering without giving up features of a system you own.

*The EULA says Sony-BMG will never be liable to you for more than $5.00... No matter what happens, you can't even get back what you paid for the CD.*

Description of Sony's
All encompassing user agreements like the one Sony includes with their rootkit-infected music CDs are not consumer solutions; they limit Sony's damages to less than $5.00 per disc, restrict whether or not you can move you computer out of country with their music on the hard drive, and force you to delete their music if you declare bankruptcy, but do nothing to protect the consumer. There are questions about how far outside the bounds of relevancy a company's user agreement can reach. Notification of privacy violations are not the solutions; control over the violations are.

Sure, changes have been made to address this problem by companies like Microsoft in regards to WMP, but Sony's recent actions have made the holes in our system glaringly obvious, and the need for public debate increasingly crucial.

date posted: 10:16 AM Fri Nov 18th, 2005
last revision: 01:02 PM Fri Nov 18th, 2005

<table>
<thead>
<tr>
<th>Sony PlayStation PSP System</th>
<th>Sony Slim Playstation 2</th>
<th>Microsoft Xbox 360 System</th>
<th>Microsoft Xbox Video Game</th>
</tr>
</thead>
<tbody>
<tr>
<td>Price: $207.95</td>
<td>Price: $129.95</td>
<td>Price: $</td>
<td>Price: $129.95</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sony PlayStation PSP System</th>
<th>Sony Slim Playstation 2</th>
<th>Microsoft Xbox 360 System</th>
<th>Microsoft Xbox Video Game</th>
</tr>
</thead>
<tbody>
<tr>
<td>Price: $207.95</td>
<td>Price: $129.95</td>
<td>Price: $</td>
<td>Price: $129.95</td>
</tr>
</tbody>
</table>

Click images for larger version