

# What's behind the rash of employee cybersnooping?

Jay Cline

July 17, 2008

It seems like a month doesn't go by anymore without news of another celebrity's personal data being peeked at by some employee at some workplace where the files are kept. It's news when [Britney Spears](#)' hospital records or [Barack Obama](#)'s passport files get perused. But do these incidents represent a growing risk that privacy and security officers need to move up on their agendas?

Certainly we're hearing about more of these incidents. Among the more recent ones:

- In July, the [State Department](#) reported that employees had accessed nine "high-profile" passport files -- including those of Obama, [Hillary Clinton](#), [John McCain](#) and Anna Nicole Smith — more than a hundred times. A subsequent audit of the files of 150 celebrities revealed that during the past six years, 127 of them had been accessed more than 4,000 times total.
- In May, five IRS workers were charged with computer fraud and unauthorized access to tax files beginning in 2005.
- The same month, a TV news anchor in Philadelphia came under investigation for allegedly reading the private e-mail of his co-anchor for several years.
- In April, the UCLA Medical Center detected that different groups of employees and unauthorized doctors since 1995 had been accessing medical records of celebrities such as Tom Cruise, Farrah Fawcett and Spears. At least one of the employees has been indicted for selling the data to media outlets.
- In February, Wisconsin utility giant WE Energies learned that employees had been routinely accessing customer information of local celebrities and others as far back as 2004.

But is there truly more employee snooping, or just more reports of it? One perspective says that we're hearing about more of these incidents because

we're getting better at detecting them — not necessarily because they're increasing in number.

Advocates of this point of view cite three recent developments: the PCI Data Security Standard has prompted an increase in system logging and monitoring, corporations and academia have boosted their deployment of privacy breach-response plans to comply with various states' breach-notification laws, and federal agencies have done likewise to comply with a directive promulgated in the aftermath of the Department of Veterans Affairs laptop breach.

These are compelling points, but I don't agree with the conclusion.

If you look at the details of the cases above, they don't appear to be the result of improved execution of privacy breach-response plans. Rather, the perpetrators are getting busted by auditors and the data subjects themselves.

I do think there's more snooping going on. In June, Cyber-Ark Software Inc. released a survey of 200 IT professionals attending an Infosecurity Exhibition Europe conference the previous month. One-third admitted to using their system access to peek at other employees' personal information.

What I think we're witnessing is the Facebook factor. This is what happens when a critical mass of people has become desensitized to browsing the intimate personal details of friends, loose acquaintances and complete strangers -- so desensitized that it no longer seems unethical for them to do the same thing with their access to confidential information systems at work.

So what if there *is* a growing trend in employee snooping; does it amount to a big deal for your company? On the Richter scale of privacy breaches, peeking at Obama's passport doesn't seem to register. These errant employees are usually authorized and trained users, after all. And most of the time, they don't appear to sell the celebrity data or use it for identity theft. No harm, no foul, right?

The celebrities and their well-financed attorneys might not agree. Celebrities may be ready to fight for what remaining privacy they have. If there is undetected celebrity snooping going on inside your walls, this is a material risk worth managing.

But the bigger risk might be what happens afterward: heightened scrutiny of all of your organization's data practices. After Pfizer's first laptop incident last summer, for example, the dominoes started to fall, one after the other, in a series of subsequently publicized breaches.

So how can you combat this threat?

It doesn't hurt to ask employees to report suspicious behavior of fellow employees. But don't depend on this alone. Oftentimes, file snooping is a group activity. And, unless an employee can be assured that his reporting of an abuse of access privileges will result in the perpetrator getting fired, he may not want to risk being discovered as the narc.

I think the best control is the blocking and tackling we should have been doing all along -- logging and monitoring. Not necessarily monitoring all systems, but those known to contain the most sensitive information and information of high-wealth individuals. The State Department reportedly had started down this path by flagging the passport files of 500 high-visibility people but apparently didn't have correspondingly tight monitoring of the access activity to those files.

If you want to offer your VIP customers enhanced privacy protection, here's a game plan that covers both sides of the coin:

- Flag your VIPs in the database, and then limit who can service and query those accounts to a subset of those with access to the full database.
- Establish tighter parameters for how frequently those accounts can be accessed and queried before an alert is sent to the information-security team.
- Perform regular spot checks of the logs for the VIP accounts to determine if any unusual activity flew below the radar of the alert parameters.

- Adopt a "one strike you're fired" policy for abuse of VIP account privileges, but provide "good driver" bonuses to those who keep a clean record.

By developing this kind of targeted discipline around logging and monitoring of VIP accounts, you might just find that it doesn't take much to scale this for all of your customers.

*Jay Cline is a former chief privacy officer at a Fortune 500 company and is now president of [Minnesota Privacy Consultants](#). You can reach him at [cwprivacy@computerworld.com](mailto:cwprivacy@computerworld.com).*