Mitchell's Musings 12-8-14: A Walk on the Sony Side of the Street for Some Private Employees

Daniel J.B. Mitchell

You have by now heard about the hacking into Sony's computer systems, essentially shutting down those systems and stealing data including video of new and unreleased movies. Some of the stolen information has been put online.

In the wake of the Sony attack, the FBI issued a private warning to companies… to be on the lookout for a certain type of destructive malware that can make data on hard drives inaccessible, according to someone who had seen it. Retrieving any data from an affected hard drive can be quite difficult and costly, according to the FBI warning…

Employees at the Sony Corp.-owned studio behind "The Amazing Spider-Man" and hit TV show "The Blacklist," have been forced to work with cellphones and personal email accounts since images of a skull appeared on company computers last week along with the message "Hacked by #GOP." Employees were warned by Sony not to use any digital devices connected to its internal networks. The hacker group, known as "Guardians of Peace," hasn't revealed any details about its identity or provided Sony with a list of demands…

There is speculation in the article cited above that the attack came from North Korea, possibly because its leader was insulted in a Sony movie.[1] I have no idea if that suspicion is true, others have raised doubts, but the focus in the news media has been on videos that were pirated and now are being circulated on the web and on the North Korean angle. Secondarily, there has been concern about cyber security in general. And finally, there is interest in the idea of Sony employees having to revert to non-Internet technology and, presumably, the lost productivity therefrom.

At the bottom of the list of interests is the information on employees that appears to have been stolen:

Several files being traded on torrent networks seen by this author include a global Sony employee list, a Microsoft Excel file that includes the name, location, employee ID, network username, base salary and date of birth for more than 6,800 individuals.[2] [Underline added]

The public radio program "Marketplace" did report on the employee data aspect and a cyber-security expert who was interviewed said in passing on the broadcast, "*You know, what employee wants their salary leaked out to the world like that?*"[3] In general, however, the employee angle was not a central focus of the media coverage of the Sony hacking and the (self-evident) idea that employees might not like to have their salaries made public seems confined to the Marketplace interviewee.[4] Of course, not only would employees not want to have their salaries made public, you can bet that Sony doesn't want its salary data out there. Such data are competitive information and could lead to raiding by other firms

[1] http://online.wsj.com/articles/more-signs-north-korea-may-be-behind-hacking-of-sony-pictures-1417467267
[2] https://krebsonsecurity.com/2014/12/sony-breach-may-have-exposed-employee-healthcare-salary-data/
[3] The comment is not in the written transcript – perhaps not considered important enough - but you can hear the full broadcast at http://www.marketplace.org/topics/tech/no-north-korea-probably-not-behind-sony-hack and find the comment at around minute 2:20.
[4] As in much of the reporting on the Sony incident, it is unclear which employees had their information stolen. Some reports suggest it was managerial employees. Others don't specify.

and internal demands to remedy perceived salary inequities. Indeed, many private employers have (legally suspect) personnel policies barring employees from discussing their salaries.[5]

What's interesting about the comment said in passing on Marketplace is that no distinction was made between types of employees. In particular, the comment is equally applicable to private sector employees – such as those of Sony – and to public sector employees. Public sector employees don't want their salaries leaked out to the world any more than private. Public sector employers have the same concerns as private, although they are less likely to have personnel policies banning employees from discussing their pay among themselves.

The difference between public and private is that thanks to court decisions, public sector salaries aren't leaked out by hackers. No hackers, whether North Korean or other, are needed. Instead, government employees' salaries are deemed to be public information and not just for top officials and executives. All public employees and their salaries down to the lowest paid and those employees otherwise not key to any public policy debate are included on open Internet sources run by various sources including newspapers. No newspapers, however, put their own payrolls online even though, of course, they have the data.

As pointed out in earlier musings, making such information available by name risks ID theft for the individuals included. While there is an argument to be made for providing such data for top government executives and officials, there is little that can be learned from the data for others that couldn't be learned by simply reporting pay by job title *without the name*. If, for example, you wanted to compare public vs. private pay, you don't need the name. Yes, in theory, one could always have gone to city hall and requested to see what John Doe or Jane Doe was being paid. But it was a bother and the information by name was thus not available at the click of a keystroke.

Courts seem not to understand that the degree of availability matters and that rules about what is public were made at a time when ease of availability online didn't exist. If for some reason there was a real public interest in a specific employee's pay – say John Doe or Jane Doe had been involved in a crime – a news reporter could obtain the information. Most people were not about to make a trip to city hall to peruse salary information. They were not about to write a letter to city hall requesting the information.

Privacy advocates ought to be raising a fuss about this issue. The rules could be different; they could be updated for the reality of the Internet. Indeed, even under current rules, not everything that could be made available is made available. For example, you could argue in theory that public employees' health records should be available on the Internet. Someone might be interested in whether John Doe or Jane Doe was driving up health insurance costs for his/her government employer because of some medical condition. But no one makes that argument in practice and in fact health records are protected on privacy grounds.

There are numerous other examples in which the Internet has developed faster than the law and a review is warranted. What's not good for Sony is not good for other employers and employees, private or public.

[5]Such policies tend to violate the protections of "concerted activity" by employees found in the National Labor Relations Act, as amended. (Supervisors and managers are not protected by the Act.)