Written by **Steven J. DuBord** on August 27, 2009

State Department Passport Snooping & RFID

A sixth U.S. State Department employee or contractor has pleaded guilty to illegally looking at electronic passport files, the U.S. Department of Justice said.

"Karal Busch, 28, of District Heights, Maryland, pleaded guilty Wednesday in U.S. District Court for the District of Columbia to one count of unauthorized computer access," *PC World* reported on August 26. "She is scheduled to be sentenced on Dec. 15."

Busch was a citizens services specialist in the Office of Children's Issues between June 2003 and July 2006, a DOJ press release stated. Busch's guilty plea said she accessed the State Department's Passport Information Electronic Records System (PIERS) and other agency databases. PIERS is the electronic repository for names, birth dates, places of birth, current addresses, and other personal data from passport applicants. Under the U.S. Privacy Act of 1974, PIERS can be accessed for official government business and nothing else.

The DOJ says that, beginning in March 2004 and ending in June 2006, Busch entered PIERS and looked at the passport applications of more than 65 celebrities and their family members, including actors, athletes, musicians, models, and others. Busch had no government business that would have authorized her access; her sole purpose, according to the DOJ, was "idle curiosity."

PC World notes that Busch is just the latest in what is becoming a long line of State Department snoopers: "Between last September and earlier this month, five other State Department employees or contractors have pleaded guilty to passport snooping charges. The three men who have been sentenced have received probation, plus community service or fines."

On August 17, Kevin Young, a contact representative, pleaded guilty to unlawfully accessing more than 125 passport files. Young's sentencing is scheduled for December 9. William Celey, a file assistant, pleaded guilty on July 10 to illegally accessing over 75 passport files. Celey is scheduled for sentencing on October 23.

But these people all appear to have done their snooping through direct computer access. Even more unnerving is the ability to get some of the same information wirelessly through the air by remotely reading the computer chips embedded in passports and other identification documents.

Thanks to the Western Hemisphere Travel Initiative, radio frequency identification (RFID) chips became

mandatory on June 1, 2009 for identification documents used by Americans entering the United States by land or sea from Canada, Mexico, or the Caribbean. Conventional passports will still be valid until they expire, but RFID chips will be the norm after that.

The new ID options all feature some form of RFID tag. There is the chipped "e-passport" and the electronic PASS card: a credit-card sized ID that includes the owner's photo and can be scanned through a pocket, wallet, or purse from 30 feet. Travelers can also use the so-called enhanced driver's licenses (EDLs) being issued in Washington state, Vermont, and Michigan; and New York. Arizona, and Texas have also signed agreements with the federal government to "enhance" their licenses. Florida and Kansas are in the process of working with the Department of Homeland Security to consider following suit.

Now what is so scary about speeding up the process of identifying travelers? Watch a YouTube video by "ethical hacker" Chris Paget to find out. It's called "Cloning passport card RFIDs in bulk for under $250":

AP said on July 11 that Paget's experiment "demonstrated something privacy advocates had feared for years: That RFID, coupled with other technologies, could make people trackable without their knowledge or consent." Not to mention vulnerable to cyberpickpockets who can wirelessly steal their credit card and ID info.

So six government employees using their computer terminals to access the PIERS database, while serious enough in its own right, pales in comparison to the snooping that computer hackers and government officials will be able to get away with thanks to RFID.