

<http://writ.news.findlaw.com/ramasastry/20060417.html>



Can States Legally Put Residents' Social Security Numbers and Other Identifying Data Online? The Troubling Answer Is That They Can, and Do

By [ANITA RAMASTRY](#)

Monday, Apr. 17, 2006

Just last week, a news report indicated that in Broward County, Florida, sensitive personal information about former and current county residents is available online -- as part of public records, such as property records, posted on [the county's website](#), which can date back to 1978.

And Broward County is hardly alone: Information on what may literally be millions of past and current residents of counties throughout Florida is also available on the Internet. This information may include Social Security numbers, driver's license numbers, and bank account details - precisely the kind of information useful to identity thieves.

The reason for this troubling situation is that Florida - like many other states - has laws requiring that public records be available to the public, and that many of them be available online.

In this column, I will urge that states with these laws need to update them to require the removal of sensitive data before records are posted online. I'll also discuss two occasions, in Ohio and Virginia, in which residents have gone to court to try to protect their Social Security numbers from public disclosure.

Electronic Public Records: Changing the Way We Access Information

In general, court and property records should remain public - as has traditionally been the case in the United States. Public records laws aid freedom of the press and instill confidence in government - allowing us to ensure, for example, that judges are not wrongly favoring certain parties. But with the advent of the Internet-- and the ability to digitize records and make

them available electronically (and searchable) - public records law must change.

[Column continues below ↓](#)

Now, an identity thief can access millions of records with the click of a computer key, from the comfort of his home, and even from abroad. Previously, he would have had to travel to the relevant office, forage laboriously in dusty archives, and examine records one by one.

Commercial data brokers, too, are accessing this information via computer - and that allows them to rapidly and easily compile personal dossiers on most Americans.

Land records are public all over the country. In addition, electoral rolls, court records, and occupational licensing records are often available online. Moreover, bankruptcy records, family court records, and even civil litigation records are in the process of going online too.

These records may include not only Social Security numbers, birthdates, and financial information, but also sensitive medical data and financial records (relevant evidence in, for example, a divorce proceeding). They may also contain ways to bypass obstacles that could otherwise confound identity thieves, and forgers - such as images of signatures, passport numbers, and green-card details.

Redaction Is Needed to Protect Sensitive Personal Data and Defeat Identity Thieves

Redaction - the removal of sensitive information - is the only solution here, and one that legislatures ought to opt for as soon as possible. Fortunately, some states are beginning to call for redaction prior to online posting. And other states exempt certain categories of records from being published online.

Similarly, state court systems are developing rules for redaction of sensitive information from their records. In Florida, for example, certain documents recorded after June 5, 2002 -- such as military discharges, family court records, and juvenile court records, wills and other probate documents and death certificates-- are automatically exempt from the public record laws. Unfortunately, the same information recorded prior to the June 2002 cutoff has or can be posted on the county site.

Also in Florida, a new statute -- set to take effect Jan. 1, 2007 -- will require county recorders to remove Social Security numbers, bank account numbers, and credit and debit card numbers from public documents before posting them on the Internet. Unfortunately, in the meantime, documents will apparently continue to be posted as is.

Redaction of sensitive information from public records may also be available upon written request, in some states or counties - such as in Broward County, Florida. But the requirements are unduly burdensome: In Broward County, a request must specify the number of the page to be redacted, and the agency that has the records. Yet the records may stretch back more than 20 years! And of course, a person has to first know that the records are available online before being able to make such a request.

Automatic redaction of certain high-risk categories of personal data is a better solution. Granted, it may be costly. But costs can be minimized on an ongoing basis by putting the burden on individuals (or their attorneys) to fill out two types of records - one with the redactions already completed, ready to be posted online.

Kentucky already has this type of dual-paperwork system, though it is administered by the government: A 30-year-old state law requires the Secretary of State to withhold Social Security numbers from all public-record business records. (In case a Social Security number is needed for identity verification, Kentucky keeps an original record with Social Security numbers intact.)

An Ohio Suit: Challenging Public Disclosure of Social Security Numbers

In early March, an Ohio man filed a class-action lawsuit against Ohio Secretary of State J. Kenneth Blackwell for posting his and other residents' Social Security numbers for years in records on a publicly searchable state website.

The records show retail purchases of certain high ticket items such as boats, garden tractors, or furniture that are purchase on credit or with loans; such purchases are often registered with the state using Uniform Commercial Code (UCC) filings, which show a lien on the items purchased on credit. The Ohio Secretary of State posts the UCC lien filings online. Some of the UCC filing statements include borrowers' Social Security numbers.

The attorney in the suit, Christian Jenkins, argued that the UCC filing forms ought to - and do not -- make clear that listing one's Social Security number is optional. The suit also claimed that the postings violated Ohio citizens' rights to privacy. Plaintiffs sought to have such information permanently removed from the site and from other publicly-available records in the agency's offices.

Blackwell eventually settled the suit and has agreed to remove social security numbers from current and future postings. Further work remains to be done, however. Ohio needs to amend certain laws that require that Social Security numbers be included on various government documents as a means of identification.

Interestingly, the Ohio Attorney General sided with the plaintiffs in the suit: He also believes that the Secretary of State's practice violated Ohio's constitution.

Generally, plaintiffs seemed to be on solid ground, legally. In numerous cases, the Ohio Supreme Court has ruled that residents have a right of privacy related to their Social Security numbers, and that their release by a public office is prohibited by federal law. In addition, an Ohio state court recently emphasized that public records custodians should redact Social Security numbers from otherwise public records before disclosing them.

A Virginia Defense: An Individual Refuses to Provide His Social Security Number

More generally, individuals can simply refuse to ever provide their Social Security Number to government entities. Section 7 of the federal Privacy Act provides all U.S. "persons" immunity from disclosing their Social Security number to any federal, state, or local government agency -- unless there is specific authority from Congress allowing the agency to require disclosure.

Virginia resident Mike Stollenwerk - representing himself - [successfully asserted this right](#) in 2003 when he went to court to defend his decision not to put his Social Security number on a concealed-handgun permit. A sheriff's deputy had asked the court to order Stollenwerk to defend his action (via a motion for an order to show cause why he should not be forced to put the number on the permit). Stollenwerk's defense was successful.

Counties that Do Post Private Information Risk Having to Pay Damages Awards

In the end, if publication of personal data on the Internet causes harm, counties may well find themselves held liable for the damages - just another reason for them to amend their public records laws as soon as possible.

For example, in 2003, [the New Hampshire Supreme Court ruled](#) that commercial data brokers can be held liable for injuries caused by their sale of sensitive personal information, such as Social Security numbers.

The case, *Remsburg v. Docusearch*, was filed after a man murdered a woman whom he had obsessed over since high school. He located her through information he received from an online investigative company. He subsequently visited her place of employment; and murdered her.

But the facts need not be so dramatic, for counties to be liable. Credit card companies may get tired of contractual bearing the burden of paying for identity theft, and may start to go after the counties that, with their websites, are making identity thieves' lives easier. And individuals who lose money, or

suffer inconvenience, from identity theft - a topic I discussed in [an earlier column](#) - may go to court to argue that the counties that are recklessly posting their private information ought to pay the tab when thieves predictably use that information to steal from them.

Anita Ramasastry is an Associate Professor of Law at the University of Washington School of Law in Seattle and a Director of the Shidler Center for Law, Commerce & Technology. She has previously written on business law, cyberlaw, and other legal issues for this site, which contains an archive of her columns.

[Company](#) | [Privacy Policy](#) | [Disclaimer](#)

Copyright © 1994-2006 FindLaw