



## Can Public Data Be Too Public?

*By Russell Perkins*

Does the act of putting public records on the Web and making them more broadly and conveniently accessible make them “too public” by opening them to casual browsing and easy searching?

On first examination, the answer seems obvious. After all, a public record by definition is a record available to the public. How can more convenient public access to public information be a bad thing? Some groups, including privacy advocates, law-enforcement agencies and other public officials, think that unrestricted Web access to public records may not be a good idea. The term used to describe the state of public records data right now is “practical obscurity.” The term comes from the U.S. Supreme Court, in an opinion upholding the FBI’s refusal to make public a rap sheet on an individual.

Although the rap sheet contained only public information, it had been compiled from public records of several states and was thus deemed too intrusive. The Supreme Court

justices concluded, in essence, that multiple public records combined together may yield a private, non-public record.

### **Building National Databases**

Access to state drivers’ license files has been a subject of debate for years. The most recent protests centered on a private company’s efforts to build a national database of individuals with names, addresses and even photographs obtained from these files—all in the name of creating a service to help businesses reduce check and credit-card fraud.

This particular debate goes to the heart of both the direct marketing and information industries. If you deal in consumer data in any way, you’ve probably already been confronted with many of these sensitive privacy issues. Make no mistake: These issues soon will impact those who deal in business information, as well.

Already, several states are facing challenges to their Web sites that offer databases of registered professionals such as doctors and accountants. Also, there have been significant controversies about

putting physicians’ disciplinary and malpractice records online.

Recently, the State of California halted sales of its database of 24 million birth and death records after a newspaper reported that the information was being made available on the Web by a genealogical organization. In addition to privacy concerns, there also were cries that the data may enable identity theft, since it contained information on living people.

Some people think that even restricted access to public information via the Web is a bad thing. In New York City, a non-profit group created a Web site to let voters view their individual voter registration records to determine at what polling place they were registered to vote. While this is public information, the site was lambasted for making the information available and only asking for a person’s last name and date of birth before displaying the requested information. The main criticism of the site was that by asking for only two pieces of identifying information, it was not sufficiently secure—although the entire database is open to public

inspection at the Board of Elections physical offices, with no identifying information being required of the petitioner at all.

The issue is compounded when public record databases not only are made accessible but merged together, creating even more powerful sources of information. In the eyes of some privacy advocates, this further erodes personal privacy.

As Charles Davis of the Freedom of Information Center at the Missouri School of Journalism puts it: “We’re equating ease of access with privacy, and to me, they’re two different animals. Either a record is private or it’s not.”

At a certain level, this is true. Yet as we’ve seen, the Supreme Court has said that multiple public records combined together may yield a private, non-public record. And when public databases are overlaid on commercial databases, the issue gets even more problematic. For example, there are databases that reside in that murky area between public and private, an area inhabited primarily—and quite profitably—by mailing lists. It wasn’t long ago that the IRS was found to be renting mailing lists of luxury-goods buyers just to see if their reported incomes could support such expensive purchases. Does this constitute sophisticated law enforcement or an invasion of privacy?

### **What’s a Good Marketer to Do?**

What’s clear is that the compilation, manipulation and distribution of data is coming under greater levels

of scrutiny, and the consequences of what you, as a marketer, do are increasingly being called into account. You must be ready with thoughtful policies that go beyond just the letter of the law, because current regulations never anticipated our ability to assemble and merge so much information together and make it easily searchable. When the aggregations of data meet the Web, such globally convenient access ultimately may lead to unintended, even criminal, consequences. Indeed, it will take time until we, as a society, can strike the proper balance.

*Russell Perkins is president of the Perkins Group, a direct marketing consulting company based in Philadelphia. He assists companies in their efforts to tackle e-commerce. You can reach him at (215) 735-8900, ext. 250, or by e-mail at [rperkins@perkinsgroup.net](mailto:rperkins@perkinsgroup.net).*

© Copyright 2004 North American Publishing Company. All Rights Reserved.