

Copyright 2000 American Lawyer Newspapers Group Inc.
Legal Times

October 30, 2000, Monday

SECTION: POV; Pg. 70

LENGTH: 1554 words

HEADLINE: Need to Know

In the rush to protect privacy online, Americans must not forget the very real benefits of public access to information.

BYLINE: Charles T. Pinck

BODY:

Recently, I was contacted by a person whose aunt had died suddenly under mysterious circumstances and had left her multimillion-dollar estate to a much younger person whom she had known only a short time. I run an investigative services firm. My new client was very suspicious that this younger person had exerted undue influence over the aunt and possibly played a role in her death. But without any actual evidence she couldn't convince the police to look into the matter.

So I ran a database search available to licensed investigators to find the younger person's address history and Social Security number. And what I learned was that the deceased aunt's name and Social Security number were connected to this person's home address—a possible indication of credit card fraud. Armed with this evidence, my client was able to persuade the police to take up the case.

As an investigator who specializes in the use of online resources, I do this kind of work all the time. Sometimes the clients hire my firm directly; sometimes we're hired by the clients' lawyers. And now in the name of privacy, lawmakers are threatening to stop these database searches.

With the explosion of the Internet and the ever-increasing sophistication of computer technology, safeguarding personal privacy has understandably become a critical issue. New laws to protect personal information are being introduced on the state and federal levels at a frenzied pace.

Many of these laws, proposed and already enacted, are reasonable. I'm well aware of the incredible amount of information available over the Internet and the potential for misuse. New statutes that address the collection, use, and dissemination of personal information in order to protect individuals against identity theft and related crimes are needed.

But as I watch the concern about privacy ratchet up, I'm troubled that these efforts to protect personal privacy will soon restrict access to previously public information. Such information is absolutely crucial to professional investigators. And investigators play an important and often unheralded role in our legal system.

The Truth Is Out There

Professional investigators access personal identifying information from database companies that require every investigative agency to provide proof of licensing and to abide by specific rules for its use. We use this information in many ways: to prevent and investigate fraud and other criminal acts; to find stolen and misappropriated assets; to enforce judgments and locate people seeking to avoid paying child support and other debts; to investigate the theft of

Need to Know In the rush to protect privacy online, Americans must not fo

intellectual property; to find witnesses; to conduct due diligence and background searches; to assist in litigation; and to discern the truth in a variety of other matters.

Personal identifying information is critical every time a licensed investigator must determine the correct identity of an individual or verify that documents refer to a specific individual. This is typically accomplished by matching a name with an address, Social Security number, or date of birth—commonly referred to as "identifiers." Imagine the difficulty in finding, say, one particular Michael Brown absent such information.

Database searches based on identifiers, often referred to as "credit headers," are always used when searching for criminal records, perhaps the most critical aspect of many investigations. Since the only nationwide criminal record database, the National Criminal Information Center, is not open to the public, private investigators must look for criminal records jurisdiction by jurisdiction. To determine where to search, we commonly begin by putting together an address history from online sources.

For example, an individual's address history gathered online played a major role in a recent due diligence investigation. With that history, I was able to locate a criminal record that otherwise would have remained hidden. It persuaded my client not to pursue a multimillion-dollar investment with a prospective business partner. Without access to credit headers, I wouldn't have found it.

But new Federal Trade Commission regulations and two bills pending in Congress—the Privacy and Identity Protection Act (S. 2876 and H.R. 4857) and the Identity Theft Prevention Act (S. 2328 and H.R. 4311)—may soon make such searches impossible. The information contained in computer databases will be walled off, even to licensed investigators.

Under the Gramm-Leach-Bliley Act, the FTC recently issued privacy regulations, including a prohibition on the use of credit header information other than for very limited purposes under the Fair Credit Reporting Act. While a literal reading of the act does not require such a prohibition, the FTC chose to interpret it as applying to credit headers. The agency did this by reversing its longstanding position that personal identifying information contained in credit reports is not "financial." By deciding that such information—including a person's name—is "financial," the FTC is able to claim that this information must be protected under the Gramm-Leach-Bliley Act.

Back in 1997, the FTC reported to Congress that it saw no need for privacy legislation concerning credit header information. The new rule, scheduled to be implemented by July 1, 2001, would effectively prohibit most current uses of this information.

The two bills now under consideration in Congress would collectively ban the sale or purchase of Social Security numbers and require their removal from credit headers, ban the sale of credit headers altogether, and grant the FTC broad authority to make further rules regarding the use of personal identifying information.

Perhaps the most troubling aspect of the proposed Identity Theft Prevention Act is a provision that would place investigators in the same legal category as credit bureaus. This would require us to turn over our entire files upon request to suspected felons and others being investigated. Victims or witnesses, fearing retribution, would be extremely reluctant to speak with any investigator. We might even have to obtain signed permission from the individuals we investigate—an obviously unworkable prospect.

Meanwhile, the proposed Amy Boyer's Law (S. 2554), which has been inserted into a "must pass" appropriations bill, provides a better solution to this problem. It would make it illegal to sell Social Security numbers to individuals—the greatest source of misuse—but would permit continued access for licensed investigators and certain other businesses that have a legitimate need. (As of last Friday, the president was threatening to veto the appropriations bill, in part because of the Amy Boyer provision.)

Need to Know In the rush to protect privacy online, Americans must not fo

Need to Know

Severely restricting access to personal identifying information will undoubtedly aid criminals and others seeking to hide their illicit activities. It will embolden some individuals to commit even more crime, knowing that tracking them down will be that much more difficult. It will help criminals trying to conceal stolen assets and avoid prosecution. Ironically, legislation designed to protect individuals against identity theft and other types of fraud will cripple investigation of the very same crimes.

Among those hurt will be lawyers and their clients. Such laws could make the service of process nearly impossible. They'll increase the cost of hiring investigators, who will have to resort to more time-consuming, less effective, and costlier techniques.

According to The Wall Street Journal, a 1995 survey of major New York City law firms found that investigators were retained in approximately "a fifth of the firms' litigation matters . . . a 33 percent increase in the past five years." I'm confident that a survey today would find that use of investigators had risen even further.

Because state and federal law enforcement agencies are overwhelmed by their workload, professional investigators also play a critical role in supplementing their efforts.

In short, while laws designed to protect privacy and prevent identity theft are being introduced with the best of intentions, they will have damaging consequences. Americans need access to information to protect themselves, their families, and their companies.

Access to public information and the right to privacy are both hallmarks of a healthy society. Confronted by new and rapidly changing technology, we're struggling to strike a balance between these two ideals. A former high-ranking military officer (for whom I once worked) told me that phone books were not publicly available in the old Soviet Union. He also said that he would never want to live in such a society, where only the government and the police had access to information.

Americans are blessed with freedom in many different forms, including ones that we don't always recognize. Many of us take for granted the benefits of the free flow of information. We need to recognize that unreasonable restrictions placed on access to previously public information will critically impair the functioning of our legal system and ultimately our society.

Charles T. Pinck is president of the Georgetown Group. He can be reached at cpinck@georgetowngroup.com.

Art Credit

Charles Stubbs

LOAD-DATE: October 31, 2000