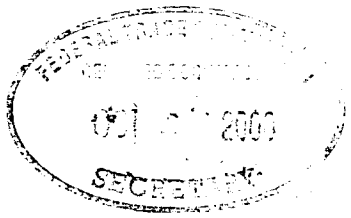


By Charles T. Pinck

With the explosion of the Internet and the ever-increasing sophistication of computer technology that can be used to gather personal information, safeguarding personal privacy has become one of the most critical issues facing our society in the new century. New laws designed to protect the collection and dissemination of personal information are being introduced at the state and federal levels at a frenzied pace. Lawmakers recognize the importance of this issue to many Americans and have begun to address it.

Many of these proposed and already enacted laws are reasonable. New laws that address the collection, use, and dissemination of personal information in order to protect individuals against identity theft and related crimes are needed. As an investigator who specializes in the use of online investigative resources, I am well aware of the incredible amount of information available through the Internet and from investigative databases and of the potential for its misuse.

As I watch the concern about privacy reach fervent proportions, I am troubled that these new laws designed to protect personal privacy will soon restrict access to previously public information. Such information is absolutely crucial to professional investigators who play an important and often unheralded role in our legal system. Professional investigators use this information in myriad of ways: to prevent and investigate fraud and other criminal acts; to find stolen and otherwise misappropriated assets; to enforce judgments and to locate people seeking to avoid paying child support and other debts; to investigate the theft of intellectual property; to locate witnesses; to conduct due diligence and background investigations; to assist in all types of litigation; and to discern the truth in a variety of matters.

This information is also critical to every situation in which an investigator must determine the correct identity of an individual or verify that documents refer to a specific individual. This is accomplished by matching an address, social security number, or date of birth -- commonly referred to as "personal identifiers." Imagine the difficulty in properly identifying an individual with a very common name absent any personal identifying data. It will make this task virtually impossible.

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 recently contacted me. My client was very suspicious that this person had exerted undue influence over the aunt and possibly played a role in her unexpected death, but she could not convince the police to investigate without any evidence.

Running a simple database search that provides a person's address history, I was able to show that the deceased aunt's name and social security number were connected to this younger person's home address – a possible indication of

credit card fraud. Armed with this evidence, my client was able to persuade the police to initiate an investigation.

Such database searches, often referred to as "credit headers," are always used when performing criminal record searches, perhaps the most critical aspect of many investigations. Since the only national criminal record database (the National Criminal Information Center or NCIC) is not available to the public, investigators must search for criminal records by specific jurisdictions. To determine where such criminal searches should be initiated, an address history is commonly requested. As part of a recent due diligence investigation, this database search enabled me to locate a criminal record that otherwise would have remained hidden. It convinced my client not to pursue a significant, multimillion-dollar investment with a prospective business partner.

Under new Federal Trade Commission regulations and an array of proposed legislation pending in the U.S. Congress – such HR 4857 (the Privacy and Identity Protection Act of 2000) and S 2328 (the Identity Theft Protection Act of 2000) – the information contained in these databases soon may no longer be available, even to licensed investigators.

Under the Gramm-Leach-Bliley Act, the Federal Trade Commission recently issued financial privacy regulations. Included among them was the prohibition on the use of credit header information other than for very limited purposes permitted under the Fair Credit Reporting Act (FCRA). This ruling was made despite the fact that the U.S. Congress, in passing this Act, did not require the Federal Trade Commission's final rule to restrict the disclosure of credit header information. The Act also included specific language designed to prevent any modification of the current interpretation and operation of the FCRA. The Federal Trade Commission chose to interpret this language in such a manner as to permit it to apply the FCRA to personal identifying information, something it has never done before.

In fact, the Commission reported to the U.S. Congress in a 1997 report that it saw no need for privacy legislation concerning credit header information. This new ruling, which is scheduled to be implemented by July 1, 2001, would effectively prohibit most current uses of this information.

Several pieces of legislation now under consideration in the U.S. Congress – S 2328, HR 4311, HR 4857, and S 2876 – 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 Federal Trade Commission broad authority to make further rulings regarding their use.

Perhaps the most troubling aspect of two bills, S 2328 and HR 4311, would force investigators to turn their entire investigative files over to suspected felons and others under investigation by placing investigators under the same legal definition as credit bureaus. Under this scenario, a witness or victim would be extremely reluctant to speak with any investigator, fearing retribution. It might

even require investigators to obtain signed permission from the individuals they investigate, an unimaginable and unworkable prospect.

Completely restricting access to such information will undoubtedly aid criminals and others seeking to hide information about themselves and their illicit activities. It will embolden criminals to commit even more crime, knowing that finding them will be even more difficult. It is ironic that legislation designed to protect individuals against identity theft and other types of fraud will cripple the ability of investigators to investigate the very same crimes.

It will affect attorneys and other professionals who rely on this information to provide the most effective, professional, and affordable legal services to their clients. These laws could make the service of process nearly impossible. Hiring investigators will become much more expensive, as they will be forced to resort to more time-consuming and less efficient investigative techniques. A provision should be made to permit continued access to this information for those individuals and entities with a legitimate need for it, with strong penalties for anyone who uses this information illegally.

Law enforcement agencies are often overwhelmed by their workload. Professional investigators play an increasingly critical role in gathering evidence in both civil and criminal matters and in supplementing the investigative efforts of state and federal law enforcement agencies.

For example, employing investigators in litigation is an increasingly common practice. According to the *Wall Street Journal*, a 1995 survey of major law firms in New York City found that investigators were retained in approximately "a fifth of the firms' litigation matters...a 33 percent increase in the past five years." I am confident that a survey taken today would find an even greater use of investigators by law firms.

Fraud is on the increase as well and here, too, investigators are often utilized to investigate such crimes. A 1998 survey of 1,200 senior executives by Ernst & Young ("Fraud: The Unmanaged Risk") found that "more than half had been defrauded in the last 12 months. 30 percent had suffered more than five frauds in the last five years." This survey also reported that "twenty-eight respondents had each lost more than $25 million...the total value of the 'worst case frauds' suffered by respondents in the last 12 months was $628 million." Eliminating access to personal identifying information will only help criminals seeking to hide stolen assets and avoid prosecution.

Individuals and corporations need access to information to protect themselves, their families, and their companies when faced with a wide array of serious or potentially serious problems. Although these laws designed to protect privacy and prevent identity theft are introduced with the best of intentions, they will have also have unintended, unforeseen, and damaging consequences.

Access to public information and the right to privacy are both hallmarks of a healthy society. Confronted by new and rapidly changing technology, we are now struggling to strike a balance between these two ideals. I once worked for a former high-ranking military officer who told me – much to my surprise – that phonebooks didn't exist in the Soviet Union (except, presumably, for party officials). He also said that he would never want to live in a society in which only the government and the police had access to information. Sadly, this is the case in much of the world.

The United States is a beacon for freedom in many different forms. Many of us take for granted the free flow of information and its benefit to our society. Unreasonable restrictions placed on access to previously public information will critically impair the ability of professional investigators and the functioning of our legal system.

The writer is president of The Georgetown Group, a Washington, DC investigative firm. He can be reached at (202) 338-4521, cpinck@georgetowngroup.com, or www.georgetowngroup.com.

The Washington Post

THURSDAY, DECEMBER 9, 1999

THE DOWNLOAD

Shannon Henry

Call Him PI Tech

The rise of the Internet has been very good for **Charles T. Pinck**, spy-for-hire.

As president of a Washington private detective firm, the **Georgetown Group**, Pinck searches for information about individuals—criminal records, mortgage loans, stock holdings—by sifting through Web sites and databases for his clients.

He used to do opposition research for political campaigns. Now, with much of the region focused on high technology instead of politics and government, Pinck's fastest-growing group of clients are venture capitalists.

Pinck says that when VCs are considering an investment, they hire him to check out the people who run the companies. He's looking for prison records, criminal cases and lawsuits, but also for evidence that the entrepreneurs owned a company before that they didn't mention (especially one with a dubious past).

And he also investigates lifestyles: Houses, boats, alimony and child-support payments, and general spending habits. He's looking to see whether they're living beyond their means, which may translate into problems with the way they run their business.

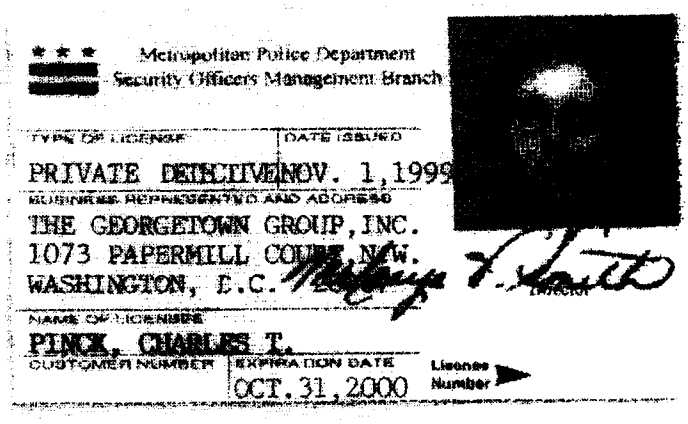
Venture capitalists, really, are sleuths themselves. They check out the technology and the books of a company before an investment. So why wouldn't they do the rest?

"Asking these uncomfortable questions are difficult," says Pinck. And the VCs, he says, are usually focused on the here and now.

"What a PI does is take a look at someone's past," he says.

Pinck says he was hired by one VC to check out a start-up the firm had decided to fund. Through public records, Pinck found that three days after meeting with the VC, the chief executive tried to get a criminal conviction for forgery wiped off the books.

See DOWNLOAD, *E11, Col. 1*



Metropolitan Police Department
Security Officers Management Branch

TYPE OF LICENSE: PRIVATE DETECTIVE
DATE ISSUED: NOV. 1,1999
BUSINESS REPRESENTED AND ADDRESS:
THE GEORGETOWN GROUP, INC.
1073 PAPERMILL COURT, NW.
WASHINGTON, D.C.
NAME OF LICENSEE:
PINCK, CHARLES T.
CUSTOMER NUMBER
EXPIRATION DATE: OCT. 31, 2000
License Number

Charles T. Pinck, president of the Georgetown Group private-eye firm, helps venture capitalists rest easier by running checks on entrepreneurs.

DOWNLOAD, *From E1*

The venture deal didn't happen, of course.

More often than not, though, the subject comes back clean.

Citing customer confidentiality, Pinck wouldn't name his VC clients, who often use his services through their attorneys.

He uses database sources that are available to many people, such as Lexis-Nexis and Dow Jones Interactive (he sometimes finds stories about a person or a previous business in a small-town newspaper).

But he also relies on subscription-based Web sites, many of which are geared toward corporate snoops like him. "Just doing a simple Internet search yields a lot," he says. Some of Pinck's favorites are KnowX.com and AutoTrackXP.com. He also likes the federal Bureau of Prisons site (*www.bop.gov*).

Most people being investigated by Pinck never know they're being checked out. He relies more on documented information than personal interviews or surveillance, what he calls "the black arts."

He does worry that new privacy laws could cripple his business. "If you enforce too many privacy laws," he says, "you're also enforcing the privacy of people who have things to hide."

• • • • •

www.georgetowngroup.com