Journal of Consumer Attorneys Associations for Southern California
ADVOCATE
November 2009 Issue

Tracy J. Hasper

The sky is falling... maybe

Legal investigators prepare for life minus one critical tool: The Social Security Number

John D. Sweeney, Jr. could not have been hard to find. The scion of a wealthy factory owner, he lived in a 15-room mansion in Westchester County, New York. Everyone in New Rochelle knew the Sweeney family. John worked as a shipping clerk at his father's factory, and it was there where he completed the application for his Social Security card. If a savvy private investigator with access to the right database could have just run that number…

In 1936, however, there were no computers and no databases of personal information. This was the dawn for Social Security Numbers. According to the Social Security Administration, John David Sweeney, Jr., 23, was the first American citizen ever to receive a Social Security card. His number, 055-09-0001, was issued in November of 1936, along with hundreds of thousands of others.

Although originally planned as an account number to track retirement contributions, the nine-digit Social Security Number, since its authorization by the Social Security Act of 1935, has become a cradle-to-grave identification number used by courts, law enforcement, hospitals, financial institutions and employers. And private investigators.

If some politicians and privacy advocates have their way, however, investigators may soon be barred from having access to Social Security Number information. These advocates argue that the identity theft epidemic, several recent high-profile cases involving investigator misconduct, and data breaches at information providers, compel government action to protect consumers. On the other side, investigators cry foul, contending that shutting them off from proprietary data bases will not only cripple their industry by compromising the services they can provide, but also seriously reduce due process for criminal defendants.

To date, this dispute has largely taken place in the legislative arena and without much media attention. Spokespeople for the investigative industry say they are frustrated that attorneys have taken little notice of the issue. Why, if at all, *should* attorneys pay any attention to the political and business problems facing private investigators? How will the proposed legislation affect the investigative function? Are there any compelling implications for civil and criminal attorneys in the quiet war being waged in Washington, D.C.?

Those in the investigative industry claim that, should the decision be made to bar them from access to private consumer information, this will result in:

• Dramatic increases in the costs of investigation;

See Hasper, Next Page

Journal of Consumer Attorneys Associations for Southern California
ADVOCATE
November 2009 Issue

• Greater delays in locating witnesses and accessing public records; and
• Decisive advantages to prosecutors and insurance defendants in litigation.

How investigators do their work

According to the U. S. Bureau of Labor Statistics, 52,000 people worked as private investigators in 2006 (the most recent year for which figures are available). Thirty percent of those were self-employed. It is safe to say that very few of them even remotely resembled the private detectives in popular imagination.

The private investigator, in popular cultural lore, is a hard-bitten, wisecracking loner who operates out of a drab office in the not-so-exclusive part of town. He reaches for his lunch in a lower desk drawer, and it usually comes in a bottle. His clients are almost always female and frequently hire him to follow their cheating husbands. He works, after collecting a healthy retainer fee, for a daily rate plus expenses. No friend of cops, the PI uses his brains, his fists, his network of smarmy informants and his Detective .38 Special to solve cases. If he needs a business card, he can choose, like Jim Rockford, from a collection of dozens in his glove box. If he needs a ruse like, say, Raymond Chandler's Philip Marlowe in The Big Sleep, he can simply don a disguise, adopt a pretext and wait for the information to flow. An array of electronic gadgets stand at his disposal: Telephone bugging devices, necktie cameras, GPS trackers, and a variety of infrared sensing devices are in the arsenal. If the infectious charm of a Thomas Magnum doesn't do the job, he can, like Mike Hammer or Robert B. Parker's Spenser, rough up an uncooperative witness.

The irony with all of this is not just that this stereotype is almost entirely fictional, but that most of the activities described here, if brought to the attention of a state licensing authority, could lead to the revocation of an investigator's license. And that's not all. If an attorney hired any investigator who engaged in violations of the requisite professional codes, that attorney might not only face a fine, but because lawyers are generally responsible for the actions of the agents they hire, could also be the target of liability lawsuits.

Part of the problem with understanding the importance of this is that those of us who practice law don't truly understand what an investigator does and how the investigative function fits into the court system. To us, it is often just one more occasionally necessary expense with which we have to burden our client.

"A lot of attorneys in private practice don't have the kind of respect for investigators that they might, and that's sad," says Katherine "Kitty" Hailey, noted author and licensed private investigator for 37 years, who now works in Philadelphia with the Federal Defender's Office, Capital Habeas Unit. "And it's not just attorneys. A lot of lawmakers, who have no idea what I do or how I do it, seem very anxious to put me out of business."

The "business" pursued by licensed investigators is best described as fact-gathering. If attorneys and judges are "triers of fact" and "finders of fact" in our justice system, investigators, acting as agents for attorneys, are the "miners of fact." They enter the rich mine fields of public records, witness interviews and Internet resources, panning for admissible evidence for use by their clients. These efforts constitute a critical element in our system. Investigators locate missing witnesses, track down hidden assets, conduct witness interviews in civil and criminal cases, uncover fraud, ferret out the hiding places of deadbeat debtors and perform a wide range of other services for their attorney clients. Contrary to the fictional image, licensed investigators must work under strict guidelines in pursuit of these goals.

During the past two decades, the work performed by investigators has been transformed by the technological advances. Relying upon public records and information extracted from consumer credit reports (not credit information, but data from what is generally termed "credit headers"), data aggregators such as ChoicePoint and LexisNexis have amassed and repackaged this information for sale to law enforcement, government agencies, insurance companies and private investigators.

This has truly revolutionized the work of investigators. What was previously accomplished only by pounding the pavement (hence the sobriquet "gumshoe"), knocking on doors, painstakingly following down leads through neighborhood inquiries, has now become immeasurably more efficient through accessing these proprietary databases.

Much of this progress can be attributed to the evolving use of the Social Security Number.

The SSN as an investigative tool

When John Sweeney was issued the "first" Social Security Number (SSN) record, the number was intended only as an account reference. There had to be some way to designate the individual account of each contributor to the Social Security system. The nine-digit geographical numbering system was the solution. Over the many decades since, however, it has taken on a distinctly different character.

As employers, hospitals, law enforcement, and government agencies (such as each state's Department of Motor Vehicles) harvested the number from consumers to satisfy indexing needs, the SSN became a personal identifier. In fact, after three-quarters of a century, the SSN has arguably become the most important number in the life of every American citizen. It is routinely offered to employers, banks, financial institutions, insurance companies, medical providers, courts, law enforcement, credit card companies, businesses and prospective landlords. A collection of business transactions and residence information becomes connected with our use of this number. Although frequently redacted now in public records, it is routinely utilized in criminal records, bankruptcy case files, Uniform Commercial Code filings, abstracts of judgment, and older vital documents, such as birth, marriage and death records. Accordingly, over the course of a consumer's lifetime, the information col-

See Hasper, Next Page

Journal of Consumer Attorneys Associations for Southern California
ADVOCATE
November 2009 Issue

lected by data aggregators, based upon the Social Security Number, constitutes a personal identifier. In fact, the Internal Revenue Service formally adopted it as the official taxpayer identification number in 1962.

Thus the Social Security Number has become a critical investigative tool and can unlock a plethora of information for the private investigator. For one thing, because it is a unique personal identifier, it allows an investigator to distinguish between individuals who share relatively common names. This is particularly important when attempting to locate and interview "missing" witnesses. If an attorney hires a private investigator to find "John Sweeney" in Los Angeles, California, the task would be daunting without more identifying information, such as a date of birth, middle name, last known address and Social Security number. In fact, a search on that name using one popular database provider, Merlin Information Services, reveals nearly 100 matches to the name. In short, the Social Security Number is the absolute identifier.

"Everything is connected to the Social Security number," said Francie Koehler, Legislative Chair with the California Association of Licensed Investigators (CALI), "and since they are pretty much the basis for everything that becomes personal information, access [by private investigators] is critical."

"It would make it far more difficult to locate persons and discern persons," said Bert Hodge, with the National Association of Legal Investigators (NALI) and a critic of moves to restrict SSN information. "There are multiple situations in which a Social Security Number is a necessary tool for distinguishing people… It's not the *be all* and *end all*, but it can sometimes be critical."

What multiple situations does Hodge have in mind? Most investigators contend that the SSN information can be indispensable in the following areas:

- Locating witnesses in civil and criminal cases;
- Investigating "grey market" activities, in which companies have sustained losses from the theft of patents and other intellectual property;
- Assisting the victims, both individuals and businesses, of identity theft;
- Locating missing persons, including heirs, critical trial witnesses, beneficiaries, debtors and "deadbeat" parents.
- Gathering physical evidence, including photographic and videographic evidence;
- Performing due diligence investigations, on behalf of corporations and businesses, regarding key personnel and executive applicants.

All of the above activities are most efficiently pursued using proprietary databases available only through established data aggregators. So, why then are some legislators so interested in closing off access to this information?

What the legislation proposes

The legislation proposed in several bills now being considered would dramatically alter the range of access to consumer information now enjoyed by investigators. The compelling interest in passing this legislation is to protect consumers from so-called "data breaches," in which sensitive information has been stolen from businesses, government entities, and data aggregators. Losses from these thefts have indeed been massive.

Victims of these data breaches during recent years have included (to name but a few) the Pentagon, the Royal Bank of Scotland, TJX, Lending Tree Mortgage Co., Hannaford Bros. Co., Certegy, Pulte Homes, FEMA, Ohio State University, George Mason University, the Georgia Department of Motor Vehicles, U.S. Veterans Administration, and data provider ChoicePoint (now part of LexisNexis). In the case of ChoicePoint, 163,000 consumer records were filched by identity thieves who established bogus accounts. In 2006, ChoicePoint paid $10 million in penalties from a settlement with the Federal Trade Commission, and $5 million to consumers for redress. According to the Privacy Rights Clearinghouse, a consumer advocacy organization, more than 252 million consumer records have been exposed to data breaches since January of 2005.

Three bills, each one seeking to restrict SSN information now available, went to committees during the 110th Congress. Each bill, in its original form, would have blocked access to private investigators. H.R. 3046, sponsored by Rep. Michael McNulty (D-NY), prohibited the sale of SSNs to the public, with exceptions for law enforcement and taxing authorities. This bill quietly went away upon Con. McNulty's sudden retirement from the House.

H.R. 948 authored and introduced by Rep. Edward Markey (D-MA) (whose Web site describes him as "a long-time privacy advocate" who wants "to introduce comprehensive electronic privacy legislation in the 111th Congress") was designed to severely restrict access to SSNs through the Internet. According to a summary of this bill, prepared by the Congressional Research Service, Markey's Social Security Number Protection Act would "make it unlawful for any person, except in certain circumstances, to: (1) intentionally display the Social Security number of another individual on a website generally accessible to the public or providing an individual with access to another individual's Social Security number through the Internet…" The "certain circumstances" constituting exemptions in this bill relate to national security, public health, law enforcement, or public health and safety. Those special circumstances do not include the needs of attorneys and private investigators. The bill is currently with the Workforce Protection Subcommittee of Education and Labor.

Finally, S. 2915, sponsored by New York Senator Charles Schumer, called for the Commissioner of Social Security to issue uniform standards for truncating SSNs. Schumer, according to Bruce Hulme, Legislative Director with the National Council of Investigation and Security Specialists (NCISS), has previously expressed concern that lack of a uniform approach to redacting the numbers has left the door open for individuals to piece together a complete number from multiple sources. This bill died in the Senate Judiciary Committee.

Not to be deterred, privacy advocates came roaring back with two new bills for the 111th Congress, both of which are wending their ways through

See Hasper, Next Page

Journal of Consumer Attorneys Associations for Southern California
ADVOCATE
November 2009 Issue

the committee process. H.R. 3306, titled "The Social Security Number Privacy and Identity Theft Prevention Act of 2009," was introduced by Rep. John S. Tanner (D-TN-8). It would prohibit the sale, purchase, and display of SSNs to the general public; however, it makes no exception for the valid use of SSNs by security professionals and investigators performing lawful work. The second bill, H.R. 122, is sponsored by Rep. Rodney P. Frelinghuysen (R-NJ-11). This bill would amend title 18 of the United States Code, and the Social Security Act, by establishing criminal penalties for the misuse of SSNs. An exception is made, in the language of this proposed bill, for "business to business" uses, a feature that investigative professionals insist must remain.

"There are two factors which explain why these sorts of bills keep coming back and why private investigators are tagged with the charge that they have misused Social Security numbers," said Hulme. "The first factor has to do with government overreaching tied in with Homeland Security and terrorism issues. The second factor is that ChoicePoint, back when all of these breaches started happening, initially came out with press releases implicating private investigators."

Private investigators? In fact, licensed investigators have been the subject of relatively few convictions for information theft and misconduct, although the cases involving them have attracted a great deal of media attention. Recent high-profile cases have involved Anthony Pellicano, the so-called "PI to the stars," and Hewlett-Packard (HP), which retained a Massachusetts-based private investigative agency to uncover the source of leaks in its Board of Directors.

Pellicano was ultimately convicted on 76 of 77 charges, including wiretapping and racketeering while, in the HP case, the company settled with the State of California in its "spy scandal," paying fines totaling $14.5 million. Other cases of misconduct by private investigators generally involve "pretexting" (extracting information by fraudulent pretense) but not the theft of Social Security Number information.

But are the major data providers actually contemplating restricting the information from private investigators? Telephone calls and e-mail exchanges, over the course of several weeks, to ChoicePoint personnel resulted in no definitive response from that division regarding whether such a change is on the horizon. However, the parent company, LexisNexis, through spokesperson David Kurt, did respond: "I'm sorry, we just have no comment on that," Kurt said.

If past performance reflects future decisions, the outlook is not good for private investigators. After the 2005 data breach, ChoicePoint severely reduced access to its personal consumer information by investigators, debt collectors, and check-cashing companies.

What will the effects be?

According to Hailey, the effects of proposed legislation could be far-reaching and crippling to the investigative industry. And the investigative industry finds itself fighting a two-front war. Not only have politicians targeted the industry for exclusion, but data providers themselves have provided indications that they will no longer give access to private investigators.

This became increasingly troubling to spokespersons in the investigative industry when, on September 19, 2008, ChoicePoint was acquired by Reed Elsevier Group plc, the British-based publisher and information provider (and parent company of LexisNexis).

"It [losing access to Social Security numbers] would be a nightmare for investigators," she says. "The perceptions people, including attorneys, have of private investigators have been formed by this ancient lore in literature, film and television. But that lore is far from the reality of how a professional investigator goes about his or her work. We're decent, hardworking, law-abiding professionals who are in the business of solving problems for our clients by getting the information they need. We can't solve those problems without having access to information. That is exactly what is at stake."

Adds Koehler, in an October 13, 2008, letter to the Federal Trade Commission, "I am very concerned that if this acquisition [of ChoicePoint by LexisNexis] is approved…without providing relief to private investigators and other consumers of these services, we and our clients will suffer irreparable harm."

But if some attorneys will face "irreparable harm," you would not know it from the level of concern expressed. The American Bar Association has not taken a position on the issue of SSN information and investigators. With some exceptions, such as former Mississippi Attorney General Michael Moore, very little concern has been expressed by those who hire investigators.

"This type of discussion has been going on since 1993," says NALI's Hodge, "and we have never been able to get attorneys interested and involved."

Contends Hailey, "My own view is that attorneys are not thinking far enough ahead about what a tremendous impact this will have. I just don't think most attorneys have really thought it through. Frankly, I don't think most investigators have."

Some conclusions

Before attorneys brush off concerns voiced by the investigative industry as mere whining, of little interest and less relevance, they ought to consider several unintended consequences:

- If some of the more restrictive bills are passed, or if data providers independently decide to eliminate an entire category of purchasers (private investigators and security companies), serious questions will arise regarding due process for criminal defendants. Do we really want to change our justice system so that prosecutors have ready access to tools which are summarily disallowed to defense investigators?
- In a larger sense, access to public records in general, and to proprietary data bases in particular, has been evolving in the general direction of more restriction. Fundamental to this evolution, however, is the fact that this restriction has affected private entities far more than government. By definition,

See Hasper, Next Page

Journal of Consumer Attorneys Associations for Southern California
ADVOCATE
November 2009 Issue

public records are records which citizens and businesses should be able to review and utilize in making decisions. Limiting access to government raises what should be worrisome questions for those interested in the free flow of information.

• If any one of these bills is passed in its current form, or if LexisNexis addresses its security problems by limiting access by private investigators, attorneys who use investigative services can look forward to dramatic increases in the costs of investigation, a reduced likelihood of recovery from debtors, advantages enjoyed by prosecutors, and dependence upon an over-burdened law enforcement to investigate claims of burglary, fire, theft, fraud, and embezzlement.

As busy as we all are in trying this case, researching that issue, managing our practices, and serving the needs of our clients, it may be in the rational self-interest of every attorney to carefully consider the unintended consequences of this proposed legislation.

Tracy J. Hasper, a California licensed attorney, is also a licensed private investigator. She is the director of investigations at Batza & Associates, Inc., a legal investigative firm that works exclusively for attorneys. She, and the investigators she manages, have investigated thousands of cases in nearly all practice areas, including serious personal injury, wrongful death, roadway and construction zone defect, product liability, employment law, class actions, civil rights, anti-trust, and criminal defense. She can be reached at thasper@batza-associates.com.