

Francis J. Menton, Jr.
391 Bleecker Street
New York, NY 10014
212-728-8246

April 11, 2000

Ms. Jennifer J. Johnson
Secretary
Board of Governors of the Federal Reserve System
20th and C Streets, NW
Washington, DC 20551

Attention: Docket No. R-1058

Robert E. Feldman
Executive Secretary
Federal Deposit Insurance Corporation
550 17th Street, NW
Washington, DC 20429

Attention: Comments/OES

Secretary
Federal Trade Commission
Room H-159
600 Pennsylvania Avenue, NW
Washington, DC 20580

Gramm-Leach-Bliley Act Private Rule,
16 CFR Part 313-Comment

Becky Baker
Secretary of the Board
National Credit Union Administration
1775 Duke Street
Alexandria, VA 22314-3428

Communications Division
Office of the Comptroller of the Currency
250 E Street, SW
Washington, DC 20219

Attention: Docket No. 00-05

Manager, Dissemination Branch
Information Management & Services Division
Office of Thrift Supervision
1700 G Street, NW
Washington, DC 20552

Attention: Docket No. 2000-13

Jonathan G. Katz, Secretary
Securities and Exchange Commission
450 5th Street, NW
Washington, DC 20549-0609

File No. S7-6-00

Ladies and Gentlemen:

Although the deadline for comments to your proposed regulations has now passed, I wonder if I might be permitted a brief response to the comments submitted on behalf of the credit bureaus. I refer particularly to the comments of D. Barry Connelly, President of the Associated Credit Bureaus, Inc., and of Oscar Marquis, Vice President and General Counsel of Trans Union. I'm sure that Experian and Equifax will also submit comments in due course, but as of this writing I have not found them on your respective web sites.

The comments of Messrs. Connelly and Marquis are breathtaking in their dishonesty. Make no mistake: this game is about one and only one thing, which the systematic theft and sale by Trans Union, Experian and Equifax of confidential information, particularly social security numbers (SSN's), sufficient to enable an investigator, or crook, to compile a complete list of every American's most private financial information. But in Mr. Connelly's 12-page letter one finds only one reference to SSN's, deftly obscured in the middle of page 2; and in Mr. Marquis' letter one must get all the way to page 9 of a 12-page letter to find a similarly buried reference to SSN's.

SSN's are:

(1) Confidential. They are available from no source other than the credit bureaus, and from them only because of blatant thievery.

(2) Financial. SSN's are the key to unlocking your financial privacy. With your name, address and SSN, I can get your bank balance, your stock portfolio, your credit card charge history, and your credit report, all without telling you I'm doing it.

In this light, let us examine some of the assertions of Messrs. Connelly and Marquis:

Connelly, page 2:

"Header information is only identifying and is devoid of any financial connotation. Examples of header information include name, address (including zip code), telephone number, year of birth, age, and any generational designation (e.g. "senior," "junior")."

Comment:

He completely omits SSN, which is the heart and soul of the so-called "credit header." Does he really think he can fool you? There is no legitimate argument that SSN is "devoid of any financial connotation." If you don't believe me, I've attached the cover story from the November 1999 Forbes detailing exactly how an investigator can strip your financial privacy once he gets your SSN.

Connelly, page 2:

"header information is generally available from other sources."

Comment:

This statement is absolutely false with regard to SSN. Secondly, there are other items not mentioned by Connelly and often used by financial institutions as indicators of identity precisely because they are non-public, which may be sold by credit bureaus as part of the "credit header." These include mother's maiden name and high school attended.

Connelly, page 2:

"For the past several years . . . consumer reporting agencies have used header information to develop valuable products and services for their customers."

Translation into everyday English:

"We're making a lot of money stealing Americans' financial privacy through selling SSN's, and we don't plan to stop."

Connelly, page 2:

"The IRS uses this information for returned mail and/or to verify Social Security numbers."

Comment:

If the IRS uses the credit header to verify SSN's, then the credit header must contain the SSN. Why can't Mr. Connelly admit this simple fact?

The IRS and the Social Security Administration (SSA) are part of the same Federal Government. In fact, they're part of the same Department - Treasury. So if the IRS needs to "verify" SSN's, exactly why can't it go across the hall in the same Department and verify the SSN's with the SSA? Because the SSA is specifically forbidden by the Privacy Act of 1974 from sharing SSN's with any other Federal agency, including the IRS. Privacy Act of 1974, 5 U.S.C. § 552a.

If SSN's are so confidential that one part of the Treasury Department is prohibited by law from giving them to the other parts, exactly how did the credit bureaus arrogate to themselves the right to steal this information off confidential credit applications and sell it to the IRS?

Marquis, page 1-2:

"In addition to the services Trans Union provides as a consumer reporting agency, we also provide a wide variety of more general information services to all types of businesses and governmental entities. For example, when state officials are having difficulty locating a parent who is refusing to pay his or her child support, they frequently came to Trans Union for a current address."

Comment

"A wide variety of more general information services" should correctly be translated as "selling stolen confidential SSN's." And what's this baloney about "they frequently come to Trans Union"? Nobody "comes to" Trans Union. Trans Union's full "credit header" data base, along with those of Experian and Equifax, containing your and my name, address, prior address, SSN, and possibly mother's maiden name, is available 24 hours a day, 7 days a week, on millions of desktops across the country, through some 15 or more "look up" data base services. Most charge \$1 per minute for as many SSN's as you can look up.

Might somebody be looking up an SSN for legitimate purposes, like chasing child support? Of course it happens. It equally happens that people look up SSN's in order to engage in identity theft or to find out your bank balance. And the credit bureaus have no control over this situation whatsoever. It's a huge disaster waiting to happen.

Marquis, page 9:

"In addition, we urge the Agencies to provide examples of the types of information excluded from the definition. These examples should expressly clarify that names, addresses, telephone numbers and **other similar information** are not covered by the definition. If such information were covered, the Proposal could have especially troublesome unintended consequences for consumer reporting agencies like Trans Union and the many businesses who rely on us for critically important information."

Comment

Is there any real doubt about what he means by "names, addresses, telephone numbers and other similar information." He's trying to slip SSN's past you by not mentioning them by name. I hate to say it, but these credit bureau guys think you Federal bureaucrats are really stupid. If they can only trick you into thinking SSN's are just like names and addresses, they're home free. Please, please, please don't be fooled. SSN's are not at all "similar" to names and addresses because they are confidential and because they can be used to steal financial identity.

The "troublesome unintended consequences" he refers to means "we won't be able to get rich selling stolen confidential information." Precisely.

On April 3, 2000 the New York Times reported that the number of cases of "identity theft" was 33,000 in 1999, up from only 11,000 two years before. Whatever they might say, the credit bureaus have no idea how many of these cases stem from their own sale of people's financial identities. Their data bases, containing the keys to everybody's identity, sit on millions of desktops. They have no way of knowing if a particular user is legitimate or illegitimate. As people figure out how this system works, the likelihood of an explosion in identity theft is enormous.

Looking at the comments you have received, is there any doubt that most were orchestrated by the credit bureaus? I find particularly obnoxious the frequent statement in the form letters that if you restrict sale of credit headers, "only criminals will benefit." The only criminals I've encountered here are Experian, Trans Union and Equifax. In 1975 I put my SSN on a confidential credit application to American Express. In 1983 I did the same at Citibank. Today, without any approval from me and over my express written objection, my SSN is for sale on a moment's notice to at least 10 million people. The culprits - Experian, Trans Union and Equifax - having been caught red-handed, claim to be the "good guys." I have no sympathy whatsoever when major corporations get caught red-handed stealing from me. Do you?

April 11, 2000

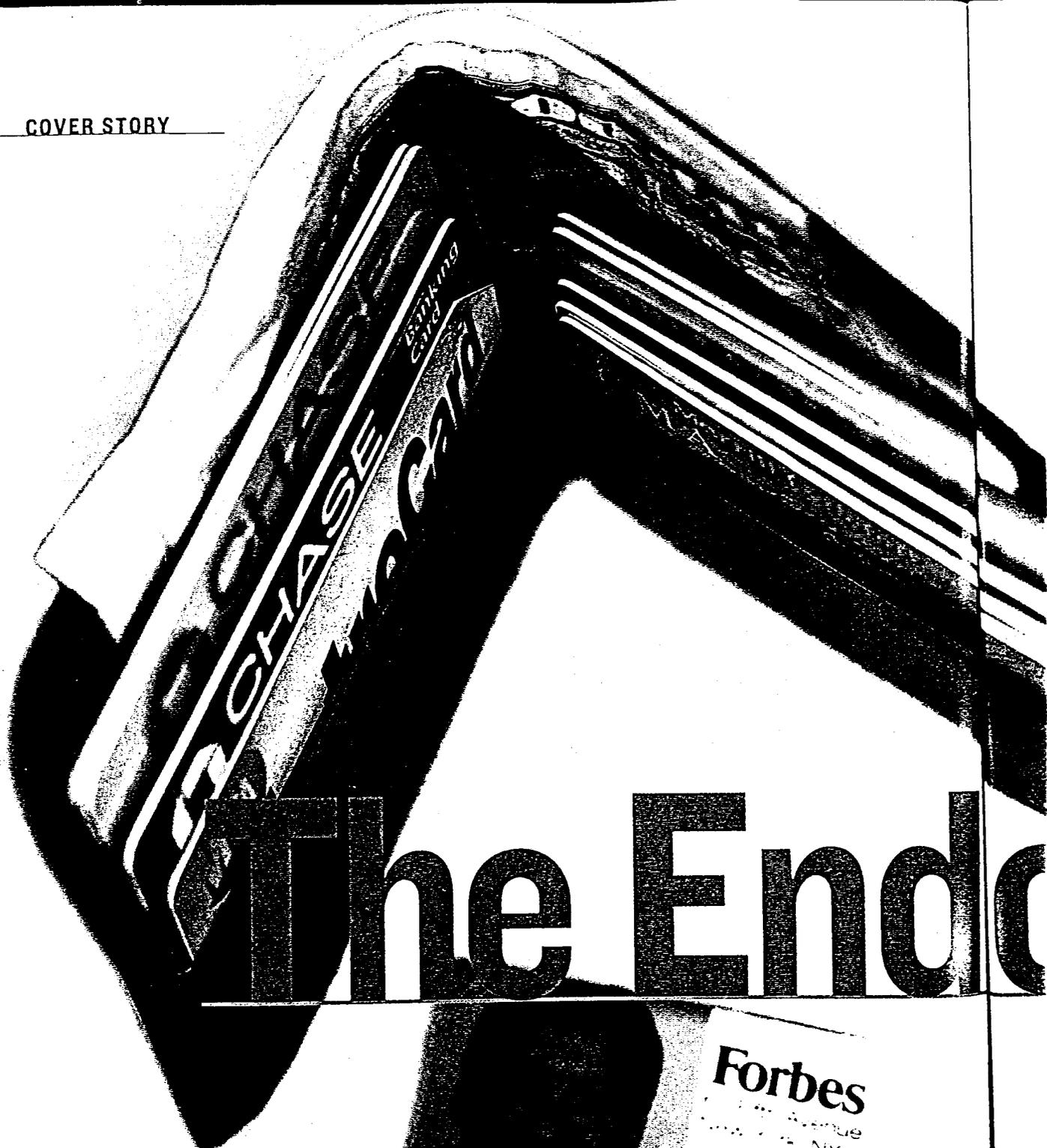
Page 6

Very few members of the general public knows what's going on here, but I can assure you that every one to whom I mention this is outraged. There may not be a lot like me to figure out the details and write long letters, but rest assured that there's a firestorm ready to blow if you continue to let the credit bureaus get away with this. The American people are counting on you!

Very truly yours,

A handwritten signature in black ink that reads "Francis J. Menton, Jr." in a cursive style.

Francis J. Menton, Jr.



The End

Forbes
200 Park Avenue
New York, NY 10011

Name	Adam Penenberg
Department	Editorial
Social Security Nbr	
Signature	<i>Adam Penenberg</i>



THE PHONE RANG AND A STRANGER CRACKED SING-SONGY AT THE OTHER END OF the line: "Happy Birthday." That was spooky—the next day I would turn 37. "Your full name is Adam Landis Penenberg," the caller continued. "Landis?" My mother's maiden name. "I'm touched," he said. Then Daniel Cohn, Web detective, reeled off the rest of my "base identifiers"—my birth date, address in New York, Social Security number. Just two days earlier I had issued Cohn a challenge: Starting with my byline, dig up as much information about me as you can. "That didn't take long," I said.

"It took about five minutes," Cohn said, cackling back in Boca Raton, Fla. "I'll have the rest within a week." And the line went dead.

In all of six days Dan Cohn and his Web detective agency, Docusearch.com, shattered every notion I had about privacy in this country (or whatever remains of it). Using only a keyboard and the phone, he was able to uncover the innermost details of my life—whom I call late at night; how much money I have in the bank; my salary and rent. He even got my unlisted phone numbers, both of them. Okay, so you've heard it before: America, the country that made "right to privacy" a credo, has lost its privacy to the computer. But it's far worse than you think. Advances in smart data-sifting techniques and the rise of massive databases have conspired to strip you naked. The spread of the Web is the final step. It will make most of the secrets you have more instantly available than ever before, ready to reveal themselves in a few taps on the keyboard.

For decades this information rested in remote mainframes that were difficult to access, even for the techies who put it there. The move to desktop PCs and local servers in the 1990s has distributed these data far and wide. Computers now hold half a billion bank accounts, half a billion credit card accounts, hundreds of millions of mortgages and retirement funds and medical claims and more. The Web seamlessly links it all together. As e-commerce grows, marketers and busybodies will crack open a cache of new consumer data more revealing than ever before (*see box, p. 188*).

It will be a salesman's dream—and a paranoid's nightmare. Adding to the paranoia: Hundreds of data sleuths like Dan Cohn of Docusearch have opened up shop on the Web to sell precious pieces of these data. Some are ethical; some aren't. They mine celebrity secrets, spy on business rivals and

1 of Privacy

Our reporter dared a private eye to dig up dirt on him. The results are terrifying to anybody who worries about prying eyes or credit card scamsters. What can you do to protect yourself?

BY ADAM L. PENENBERG

F O R B E S • November 29, 1999 183

track down hidden assets, secret lovers and deadbeat dads. They include Strategic Data Service (at datahawk.com) and Infoseekers.com and Dig Dirt Inc. (both at the PI Mall, www.pimall.com).

Cohn's firm will get a client your unlisted number for \$49, your Social Security number for \$49 and your bank balances for \$45. Your driving record goes for \$35; tracing a cell phone number costs \$84. Cohn will even tell someone what stocks, bonds and securities you own (for \$209). As with computers, the price of information has plunged.

You may well ask: What's the big deal? We consumers are as much to blame as marketers for all these loose data. At every turn we have willingly given up a layer of privacy in exchange for convenience; it is why we use a credit card to shop, enduring a barrage of junk mail. Why should we care if our personal information isn't so personal anymore?

Well, take this test: Next time you are at a party, tell a stranger your salary, checking account balance, mortgage payment and Social Security number. If this makes you uneasy, you have your answer.

"If the post office said we have to use transparent envelopes, people would go crazy, because the fact is we all have something to hide," says Edward Wade, a privacy advocate who wrote *Identity Theft: The Cybercrime of the Millennium* (Loompanics Unlimited, 1999) under the pseudonym John Q. Newman.

You can do a few things about it (see box, p. 186). Give your business to the companies that take extra steps to safeguard your data and will guarantee it.

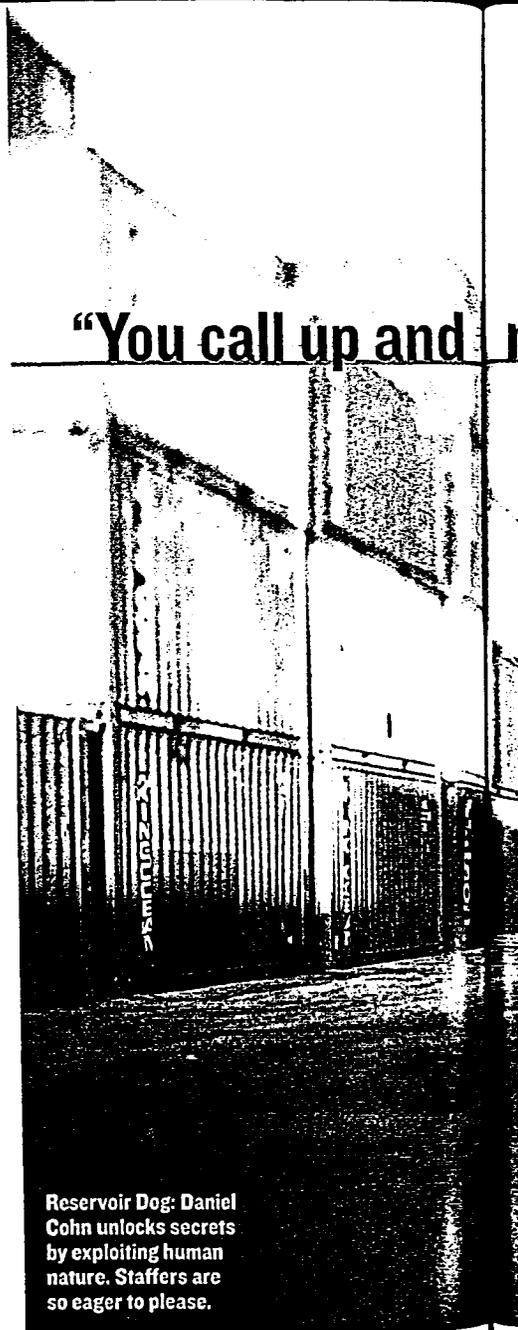
Refuse to reveal your Social Security number—the key for decrypting your privacy—to all but the financial institutions required by law to record it.

Do something, because many banks, brokerages, credit card issuers and others are lax, even careless, about locking away your records. They take varied steps in trying to protect your privacy (see box, p. 187). Some sell information to other marketers, and many let hundreds of employees access your data. Some workers, aiming to please, blithely hand out your account number, balance and more whenever someone calls and asks for it. That's how Cohn pierced my privacy.

"You call up a company and make it seem like you're a spy on a covert mission, and only they can help you," he says. "It works every time. All day long I deal with spy wannabes."

I'm not the paranoid type; I don't see a huddle on TV and think that 11 football players are talking about me. But things have gone too far. A stalker would kill for the wealth of information Cohn was able to dig up. A crook could parlay the data into credit card scams and "identity theft," pilfering my good credit rating and using it to pull more ripoffs.

Cohn operates in this netherworld of private eyes, ex-spooks and ex-cops, retired military men, accountants and research librarians. Now 39, he grew up in the Philadelphia suburb of Bryn Mawr, attended Penn State and joined the Navy in 1980 for a three-year stint. In 1987 Cohn formed his own agency to investigate insurance fraud and set up shop in Florida. "There was no shortage of



Reservoir Dog: Daniel Cohn unlocks secrets by exploiting human nature. Staffers are so eager to please.

On the Web, No One Is Anonymous

On the Web you sense that you're invisible. That probably is what David L. Smith thought. But the young geek charged with creating the Melissa virus was wrong.

Smith didn't know that Microsoft, whose office software has 100 million users worldwide, embeds a unique numeric identifier into every copy of Office 97. This ID puts a watermark on every Microsoft Office document created with this software. So when Smith surfed the Web, he left behind his code—and in essence his name. Authorities nabbed him by matching the code found in the virus to documents he had posted to a Web site frequented by virus makers.

So Microsoft may know who you are—and so might every Web

site you have ever flitted past. That's the point of "registrations" for such "free" services as e-mail and personal home pages; that's part of what inspires "cookies," the electronic eavesdroppers that track your every move to let the site serve you better (and market to you better, too).

"A profile could be created of every site a user visits, and that could be linked to that user's real-world identity—all without the user's express permission," says Barbara Bellissimo, chief executive of Privada, a Web site (www.privada.net) offering anonymous Web surfing. "Imagine a record being made of every time you walked into a store and looked around, and every time you walked by a store

and make it seem like you're a spy on a covert mission."



work," he says. He invented a "video periscope" that could rise up through the roof of a van to record a target's scam.

In 1995 he founded Docusearch with childhood pal Kenneth Zeiss. They fill up to 100 orders a day on the Web, and ex-

pect \$1 million in business this year. Their clients include lawyers, insurers, private eyes; the Los Angeles Pension Union is a customer, and Citibank's legal recovery department uses Docusearch to find debtors on the run.

Cohn, Zeiss and 13 researchers (6 of them licensed P.I.s) work out of the top floor of a dull, five-story office building in Boca Raton, Fla., sitting in cubicles under a fluorescent glare and taking orders from 9 a.m. to 4 p.m. Their Web site is open 24 hours a day, 365 days a year. You click through it and load up an on-line shopping cart as casually as if you were at Amazon.com.

The researchers use sharp sifting methods, but Cohn also admits to misrepresenting who he is and what he is after. He says the law lets licensed investigators use such tricks as "pretext calling," fooling company employees into divulging customer data over the phone (legal in all but a few states). He even claims to have a government source who provides unpublished numbers for a fee, "and you'll never figure out how he is paid because there's no paper trail."

Yet Cohn claims to be more scrupulous than rivals. "Unlike an information

window and merely stopped to look at it."

At the Dr. Ruth sex-advice service, visitors are warned that it may "relate a user's use of this site to information that the user has specifically and knowingly provided." The outlet is run by Time Inc. New Media, which promises it won't do such interpolation for kids' sites but gives no such assurance regarding adults.

Maybe it's no big deal if a Fidelity pitch shows up in your mailbox after you have hung out at thestreet.com. The problem is, where will it stop? Will an "anonymous" posting be picked up by an employer? Better to take steps to safeguard your identity in cyberspace:

- Don't give out personal information to a Web site unless it has a satisfactory privacy policy. If a Weblet won't promise to forgo sharing your file with other sites, don't go there. Alternatively, make up a

fictitious persona for use on-line.

- Don't give your credit card to unfamiliar Web sites.
- In visiting spots on the wrong side of the tracks, consider going through sites like [Privada](http://Privada.com) (\$5 a month) and anonymizer.com, which at least profess to let you surf the Net in anonymity.
- Use a free e-mail account at a site like excite.com as your return address for commercial dealings and don't worry that it may fill up with junk. Save a private account for friends and your employer.
- Create multiple profiles, each tailored to the type of site you visit and your activity there. Novell Corp. recently unveiled such a service, calling it [DigitalMe](http://DigitalMe.com) (FORBES, Oct. 18).
- Don't send anything confidential in unencrypted electronic messages.

—A.P.

broker, I won't break the law. I turn down jobs, like if a jealous boyfriend wants to find out where his ex is living." He also says he won't resell the information to anyone else.

Let's hope not. Cohn's first step into my digital domain was to plug my name into the credit bureaus—Transunion, Equifax, Experian. In minutes he had my Social Security number, address and birth date. Credit agencies are supposed to ensure that their subscribers (retailers, auto dealers, banks, mortgage companies) have a legitimate need to check credit.

"We physically visit applicants to make sure they live up to our service agreement," says David Mooney of Equifax, which keeps records on 200 million Americans and shares them with 114,000 clients. He says resellers of the data must do the same. "It's rare that

anyone abuses the system." But Cohn says he gets his data from a reseller, and no one has ever checked up on him.

Armed with my credit header, Dan Cohn tapped other sites. A week after my birthday, true to his word, he faxed me a three-page summary of my life. He had pulled up my utility bills, my two unlisted phone numbers and my finances.

This gave him the ability to map my

it's the law.) If I had an incurable disease, Cohn could probably find that out, too.

He had my latest phone bill (\$108) and a list of long distance calls made from home—including late-night fiberoptic dalliances (which soon ended) with a woman who traveled a lot. Cohn also divined the phone numbers of a few of my sources, underground computer hackers who aren't wanted by the po-

"I won't break the law. And I'll never sell

routines, if he had chosen to do so: how much cash I burn in a week (\$400), how much I deposit twice a month (\$3,061), my favorite neighborhood bistro (the Flea Market Cafe), the \$720 monthly checks I write out to one Judith Pekowsky: my psychotherapist. (When you live in New York, you see a shrink;

lice—but probably should be.

Knowing my Social Security number and other personal details helped Cohn get access to a Federal Reserve database that told him where I had deposits. Cohn found accounts I had forgotten long ago: \$503 at Apple Bank for Savings in an account held by a long-ago landlord as a

Eluding Big Brother

These words of warning may come too late to save you. Chances are, a lot of your personal information has leaked out in cyberspace and will never be purged. But you can take some steps to make it more difficult for someone to violate your future digital secrets. It's a matter of how paranoid you are and how far you want to go.

Privacy author Edward Wade has gone to great lengths to lower his profile, publishing his books under a variety of pseudonyms (*How to Investigate Your Friends, Enemies & Lovers*, by John Q. Newman). To change his data at the credit bureaus, Wade spent days filling out warranty cards, credit card applications and magazine subscriptions with hazy information. Instead of providing a home address and home phone number, he used a post office box and a voice mailbox. He never gives out his Social Security number. And when he buys big-ticket items like, say, a house or a car, Wade uses a corporation only he knows the name of as his sole contact.

"Share the spurious with the curious," he advises. Sure, it takes time and gall, but "if someone isn't important to you, do they really need to know your home phone number?" Some other tips:

1. Stop filling out as many forms as you can, and give up only the personal data that are absolutely necessary. Supermarket shopping cards, telephone solicitations, warranty cards and magazine subscriptions are an easy way for companies and individuals to collect information on you.

2. Don't write checks in stores. That provides too many details—your name, address, account number and signature—to a complete stranger. Use a debit card.



Do not disturb: Edward Wade uses pen names and a corporate shell to lie low.

3. Don't carry anything with your Social Security number on it in your wallet. It's a passkey for violators.

Those are the easy steps. Now for some hard-core ones:

4. Check the policies of the banks and brokerages you patronize—how many people can access your data, whether you are notified whenever someone checks your records or the bank gets

security deposit; \$7 in a dormant savings account at Chase Manhattan Bank; \$1,000 in another Chase account.

A few days later Cohn struck the mother lode. He located my cash management account, opened a few months earlier at Merrill Lynch & Co. That gave him a peek at my balance, direct deposits from work, withdrawals, ATM visits, check numbers with dates and amounts,

suing telemarketers for bothering him. "The two issues are knowledge and control: You should know what information about you is out there, and you should be able to control who gets it."

How did Cohn get hold of my Merrill Lynch secrets? Directly from the source. Cohn says he phoned Merrill Lynch and talked to one of 500 employees who can tap into my data. "Hi, I'm

ell your information behind your back."

and the name of my broker.

That's too much for some privacy hawks. "If someone can call your bank and get them to release account information without your consent, it means you have no privacy," says Russell Smith, director of Consumer.net in Alexandria, Va., who has won more than \$40,000

Dan Cohn, a licensed state investigator conducting an investigation of an Adam Penenberg," he told the staffer, knowing the words "licensed" and "state" make it sound like he works for law enforcement.

Then he recited my Social Security, birth date and address, "and before I could get out anything more he spat out your account number." Cohn

told the helpful worker: "I talked to Penenberg's broker, um, I can't remember his name...."

"Dan Dunn?" the Merrill Lynch guy asked. "Yeah, Dan Dunn," Cohn said. The staffer then read Cohn my complete history—balance, deposits, withdrawals, check numbers and amounts. "You have to talk in the lingo the bank people talk so they don't even know they are being taken," he says.

Merrill's response: It couldn't have happened this way—and if it did, it's partly my fault. Merrill staff answers phoned-in questions only when the caller provides the full account number or personal details, Merrill spokesperson Bobbie Collins says. She adds that I could have insisted on an "additional telephonic security code" the caller would have to punch in before getting information, and that this

subpoenaed, how you stop your information from getting sold to other marketers. Reward the discreet, and abandon those who aren't.

5. Inform your bank in writing that you don't want your records shared with anyone. "You have to do this every six months or so, but it can make the job of a dirt digger like Dan Cohn much harder," Edward Wade says.

6. Contact the Direct Marketing Association (www.the-dma.org; (212) 768-7277) and opt out of its mail-list programs. Companies constantly buy, sell and swap lists, and bailing out cuts way down on junk mail.

7. Get a nonpublished, nonlisted number. Be sure to ask for both. Otherwise, directory assistance will tell anyone who asks that you do, indeed, live in your city, but your number is unpublished.

8. Use a P.O. box or a private mail drop. Some states will let you do this on your driver's license. This cuts way down on the number of people who have your home address.

9. Use a voice-mail number for all but personal correspondence—work associates, the dentist, your mechanic. Get a pager tied to your voice mail and always be the one to call back. This will dramatically reduce the number of people who know your home number.

10. If you're really desperate, think about starting over with a new identity. At Wade's Web site (www.privacypower.com) you can get assistance with this disappearing act. "Sometimes it's easier to start over with a new identity than to fix what went wrong in their lives," the bashful author says.

But consider that only as a final option. —A.P.

How Secret?

WHEN IT COMES TO PROTECTING YOUR privacy, banks and brokerage firms tend to squirm. By law they must record your Social Security number, the marker that can unlock the data in all too many other accounts. Some institutions refuse to guarantee they won't reveal data about your account to a third party, and some won't even call you if such an outside inquiry is made.

Nor will they promise to keep your name and account out of the hands of the credit bureaus, because to get hold of bureau data they must agree to offer up their files, in exchange. One day we may grow so wary of digital intrusions that safeguarding your data will become a major point of competition for financial institutions. Until then customers must make do and distinguish the few fine points that separate otherwise boilerplate policies.

J.P. Morgan Private Banking

Takes accounts of about \$1 million and up. Won't reveal account information to a third party unless required to do so by law. Where legal, will alert the customer that somebody is snooping in his account.

Bank of America

Won't reveal account information to a third party unless required by law. Where legal, will alert the customer when someone makes an inquiry.

Wells Fargo

Won't reveal account information to a third party unless required to do so by law. Where legal, the bank will alert customer about inquiries. Says it has other ways "to verify the identity of a customer who calls asking for someone's account information."

Charles Schwab

Promises its 6.3 million customers that it won't disclose account information unless required to do so under the law. But it stops short of assuring that it will give you a heads-up if someone else tries to gain access to your account.

BankOne

Stops short of guaranteeing a third party won't get access to your account. Also won't necessarily alert you if such an attempt is made. The bank tries to ensure confidentiality, but "we can't commit because we couldn't foresee all the circumstances," says a spokesman.

—CHANA SCHOENBERGER

option was disclosed when I opened my CMA. Guess I didn't read the fine print, not that it mattered: Cohn says he got my account number from the Merrill rep.

Sprint, my long distance carrier, investigated how my account was breached and found that a Mr. Penenberg had called to inquire about my most recent bill. Cohn says only that he called his government contact. Whoever made the call, "he posed as you and had enough information to convince our customer service representative that he was you," says Russ R. Robinson, a Sprint spokesman. "We want to make it easy for our customers to do business with us over the phone, so you are darned if you do and darned if you don't."

Bell Atlantic, my local phone company, told me a similar tale, only it was a Mrs. Penenberg who called in on behalf of her husband. I recently attended a conference in Las Vegas but don't remember having tied the knot.

For the most part Cohn's methods fly below the radar of the law. "There is no general law that protects consumers' privacy in the U.S.," says David Banisar, a Washington lawyer who helped found the Electronic Privacy Information Center (www.epic.org). In Europe companies classified as "data controllers" can't hand out your personal details without your permission, but the U.S. has as little protection as China, he contends.

The "credit header"—name, address, birth date, Social Security—used to be kept confidential under the Fair Credit Reporting Act. But in 1989 the Federal Trade Commission exempted it from such protection, bowing to the credit bureaus, bail bondsmen and private eyes.

Some piecemeal protections are in

Mind Readers

Yahoo has an enviable arsenal of strengths: Twelve-month revenue exceeds \$430 million and net income has passed \$100 million; 7,500 merchants sell through the site.

So what is its "single greatest asset," in the view of Yahoo President Jeffrey Maller? The wealth of data it gathers on 80 million customers, he says—their names, their preferences online and details on which merchants they visit and what they buy. Like it or not, the very stuff that so rattles privacy advocates also makes the Web a much better and smarter place to shop—and marketers have barely begun.

Although Yahoo doesn't sell access to its 80 million sets of personal preferences and registration information, it makes hay in other ways. Leveraging the secrets it keeps, it cross-references the data to tailor pitches to users and sell, to marketers, narrowly targeted access to specific sections of its user base. "We're not trying to find out about you as an individual," says Anil Singh, Yahoo's chief marketing officer, "but if you've selected certain interests, we can extrapolate that you'll be responsive to certain other types of content and merchandising."

He takes pains to emphasize Yahoo's commitment to user privacy, but he can't help boasting about its prowess in delivering the perfect audience to advertisers. "Say you want to reach men between 24 and 35 with specific interests and a certain income level. We can put you in front of 2 million of them in the finance section," Singh says. "At the high end of our rate card, you get a type of targeting you can't get anywhere else."

Most Web marketers are wary of discussing what they hope to do with your data. Amazon.com found out the hard way in August how touchy consumers can get. Its "purchase circles,"

Head game:
Anil Singh
wants to know
you better—
much better.

Colorado is one of the few states that prohibit "pretext calling" by someone pretending to be someone else. In July James Rapp, 39, and wife Regana, 29, who ran info-broker Touch Tone Information out of a strip mall in Aurora, Colo., were charged with impersonating the Ramseys—of the JonBenet child murder case—to get hold of banking

Indeed, government agencies are some of the worst offenders in selling your data. In many states the Department of Motor Vehicles was a major peddler of personal data until Congress passed the Driver's Privacy Protection Act of 1994, pushing states to enact laws that let drivers block distribution of their names and addresses. Some states, such

At Merrill Lynch, "before I could get out anything m

place: a 1984 act protecting cable TV bills; the 1988 Video Privacy Protection Act, passed after a newspaper published the video rental records of Supreme Court nominee Robert Bork. "It's crazy, but your movie rental history is more protected under the law than your credit history is," says Wade, the author.

records that might be related to the case.

Congress may get into the act with bills to outlaw pretext calling. But lawyer Banisar says more than 100 privacy bills filed in the past two years have gone nowhere. He blames "an unholy alliance between marketers and government agencies that want access" to their data.

as Georgia, take it seriously, but South Carolina has challenged it all the way up to the U.S. Supreme Court. Oral arguments are scheduled for this month.

As originally conceived, Social Security numbers weren't to be used for identification purposes. But nowadays you are compelled by law to give an accurate



which let Web surfers learn which books were most popular at, say, a particular company, caused such an uproar that Amazon had to water down the feature days after it debuted, giving customers an option to avoid getting listed.

San Francisco-based Andromedia, acquired by Macromedia in October, sells software that compares each user's moves on a Web site with the actions of thousands of previous visitors to come up with recommendations on the fly. Chase Manhattan, E-Trade, Intuit, DaimlerChrysler and Xerox use the software to tailor their sites to the desires of each user.

Stephen Kanzler, an Andromedia vice president, says the software acts like a salesman at a high-end department store who watches a customer, then steps in to make suggestions. "If the salesman is any good, his reaction will be personalized," Kanzler says. "If he's really good, he will upsell you."

Andromedia's software records not just the preferences a user claims to have but also things like how long he or she looks at a particular product and which banner ads get clicked. As the shopper moves through the Web store, the software sifts through the files of earlier shoppers who made similar choices to offer more attractive options each step of the way. Kanzler says the software can crank out a new suggestion in less than 10 milliseconds. "We use the human brain as the pre-processor for all that info, and the brain boils it down for us: 'I liked it' or 'I didn't like it,'" he says.

Andromedia claims its customers find users sticking around 75% longer, spending 33% more money and returning twice as often as before its software was used. And who gets to own all those details about what shoppers are doing? The Web sites themselves—all to target you even better the next time around.

—JOSH MCHUGH

number to a bank or other institution that pays you interest or dividends; thank you, Internal Revenue Service. The bank, in turn, just might trade that number away to a credit bureau—even if you aren't applying for credit. That's how snoops can tap so many databases.

Here's a theoretical way to stop this linking process without compromising

need to know your credit history. It would be hard for a sleuth to know that William H. Smith 001-24-7829-33 was the same as 350-68-4561-49. Your digital personas would converge at only one point in cyberspace, inside the extremely well guarded computers of the IRS.

But for now, you have to fend for yourself by being picky about which

it. If a business without a legitimate need for the Social Security number asks for it, leave the space blank—or fill it with an incorrect number. (Hint: To make it look legitimate, use an even number between 10 and 90 for the middle two digits.)

Daniel Cohn makes no apologies for how he earns a living. He sees himself as a data-robbing Robin Hood. "The problem isn't the amount of information available, it's the fact that until recently only the wealthy could afford it.

That's where we come in."

In the meantime, until a better solution emerges, I'm starting over: I will change all of my bank, utility and credit-card account numbers and apply for new unlisted phone numbers. That should keep the info-brokers at bay for a while—at least for the next week or two. **F**

ing more he spat out your account number."

the IRS' ability to track unreported income: Suppose that, instead of issuing you a single 9-digit number, the IRS gave you a dozen 11-digit numbers and let you report income under any of them. You could release one to your employer, another to your broker, a third to your health insurer, a fourth to the firms that

firms you do business with and how much you tell them. If you are opening a bank account with no credit attached to it, ask the bank to withhold your Social Security number from credit bureaus. Make sure your broker gives you, as Merrill Lynch does, the option of restricting telephone access to your account, and use

MARK RICHARDS