Cybersleuthing for People Who Can't Set the Clock on Their VCR

"First, they do an on-line search."

Craig Ball
3402 Cedar Grove
Montgomery, Texas 77356
Tel: 936-582-5040
E-Mail: craig@ball.net
Web: www.craigball.com

Cybersleuthing for People Who Can’t Set the Clock on their VCR

It seems not a day goes by without a sensational news story on how the Internet compromises our personal privacy. A new movie cliché is the Hacker-with-a-Heart-of-Gold, a computer geek who can tap a few keys and access any database of personal information from one’s shoe size to medical history to credit card usage. The good-guy hacker is often matching wits with his corrupt counterpart in the S.G.A. (*Shady Government Agency*), a twisted cyber whiz who can instantly tap any phone or re-task a surveillance satellite. This is cybersleuthing Hollywood style. It’s mostly fantasy because much of the techno wizardry is not currently possible, at least not as depicted; but it’s also spooky because cybersleuthing already is far more invasive, revealing, and downright easy than you might expect. Nowadays, erstwhile Sherlocks can slake their thirst for detective work by getting the goods on their Moriartys online.

What is this Thing Called Cybersleuthing?

Cybersleuthing is a word I coined long ago—really at the dawn of the web--and it just caught on. It’s using the power of the Internet to gather revealing information on people and to skip trace (track someone down. For lawyers, the web is a broad avenue for informal discovery, allowing litigators to test a witness’ candor and probe a litigant’s background and resources.

> "You have zero privacy [on the Internet] anyway.
> Get over it."
> --Scott McNealy
> CEO of Sun Microsystems

Who Do You Trust?

Like salespeople, politicians and escort services, lawyers are in the persuasion business. Trial lawyers must persuade juries that their client’s interests should prevail. Jury persuasion can be based on trust or education, but most often it requires a measure of both.

Needing to build or shake trust doesn’t start and stop with the jury. The hearts and minds of the witnesses, the court, opposing counsel and those holding the purse strings are won or lost according to whom they trust and distrust.

How do you gain someone’s trust? How do you throw an opponent off-balance? How do you show that opponents or witnesses are not to be trusted? A nugget of information obtained by cybersleuthing can go a long way to accomplishing all of these tasks. Trial work entails taking sworn testimony by deposition, and not everyone honors a sworn oath. Witnesses' willingness to tell the truth is tied to their perception of the risk they will be caught in a lie. If I know something about a witness that I'm not supposed to know—something trivial, strange or obscure that didn’t emerge from the formal discovery process--the witness can’t be sure what else I know and will be less likely to stray from the truth.

The Hearing is in the Telling

Don’t wait for jury selection to start the persuasion engine. Facts may be facts, but the hearing is in the telling. Because most of what we communicate in person is conveyed non-verbally, what witnesses feel about the questioner is as much a part of the message as their words. Cybersleuthing can turn up tidbits about the witness' background that can be parlayed into rapport. For example, if a witness grew up in a small town in western Pennsylvania. I go online to find out what her folks did for a living, what schools she attended, where the local kids hung out, and so on. If the opportunity arises, I can ask, "Did you hang out at the Dairy King on Sycamore Street?" or "Weren’t they the big rivals with Central High’s football team?” and forge an instant connection with her. Obviously, this technique has to be used with discretion or you might seem more stalker than confidant.

Consider the Source

Anyone can post anything on the web, so be skeptical of information derived from all but the most trustworthy online sources until it’s verified. Uncorroborated Internet data should never play a decisive role in critical decisions like hiring, firing or leveling accusations. The sheer volume of online records, data entry errors and identity theft can lead to misidentification. I learned that lesson the hard way several years ago during a cybersleuthing presentation to a group of local businessmen. The group asked me to demonstrate Internet information gathering by assembling data about members of the audience, so I pulled up the marriage license record of the daughter of a gentleman in the front row and congratulated him on his daughter's recent nuptials. The trouble was he had no idea that his daughter was married! His daughter had an uncommon name and her birth date was a match. I was embarrassed and confused, but you can imagine how he felt! A trip to the County Clerks' office to obtain a copy of the actual document revealed that, lo and behold, there was another woman in town with the exact same name and birth date. What are the odds?! Consider the source, cross check and be careful.

The Changing Face of Cybersleuthing

Of late, fear and fortune have taken a toll on the net’s cybersleuthing resources. Fear of identity theft and cyberstalking--or fear of liability for misuse of data--prompted many excellent sites to shut down. Further, the collapse of the so-called “Internet Bubble” laid waste the notion that attracting large numbers of non-paying visitors to free sites is as valuable as cash flow. Accordingly, many free resources went dark or converted to subscription or pay-as-you-go services. Consolidation has also reduced the number of resources as larger databases purchased ailing competitors and some prominent fee-based sites restricted access as widely publicized identity theft scandals triggered unwelcome publicity.

In misguided efforts to curtail identity theft, legislatures across the nation criminalized online publication of names and “identifiers” like social security numbers and drivers licenses. Though identity theft is a genuine concern deserving legislative scrutiny, the efforts to stem identity theft by criminalizing publication of public data only serve to protect those who’ve failed to implement secure authentication mechanisms. Social security and drivers’ license numbers are inherently insecure identifiers. They’ve been widely distributed and available for years and they pervade public records of every stripe. Anyone who knows the net appreciates that data published online never disappears. It’s irresponsible for any institution obliged to guard financial or personal security to build authentication systems incorporating flawed identifiers like social security and drivers' license numbers or mothers' maiden names. These legislative efforts only serve to create a false sense of security and prolong the use of broken systems.

But while some cybersleuthing resources dwindle, new ones emerge. The explosive growth of, *e.g.,* online matchmaking services, web blogs and nostalgia sites connecting former classmates prompts many to place revealing information online. With the net's emergence as a venue for people of all ages and (to a lesser extent) all socioeconomic strata, the volume of personal data has mushroomed. Though it's still easier to gather data about persons with property and strong community ties; more-and-more, the Internet snares data about everyone.

Skip Tracing

For tracking down witnesses, defendants, agents for service and the occasional wayward client, the Internet's speed and affordability can't be beat. One hitch is that online resources primarily track middle-class and affluent Americans. Aside from convicted criminals, the Internet is not very good at finding people who actively conceal their identity, live outside the United States or cannot afford or eschew credit and other mainstream connections like driver's licenses, real estate or vehicle ownership, utility service, voter registration, web surfing and bank accounts. In that event, the best approach is to identify persons who know the subject and talk to them—people rarely sever all ties with family and friends.

> "Certainly there is no hunting like the hunting of man and those who have hunted … men long enough and liked it, never really care for anything else thereafter."
> —Ernest Hemingway
> "On the Blue Water," Esquire, April 1936

As you assemble information, make note of vital statistics and other data concerning the subject's spouse, children, siblings, parents, close friends, employers, employees, roommates, business partners, parole officers, neighbors, assumed names, etc. These collateral subjects may be easier to track and help point you to the subject.

Building on the Basics

The four primary information items for skip tracing are full name, date of birth, social security number and driver's license number. Having the subject's name and one of the other three items will almost always suffice to secure the other two. Because people are usually capable of estimating a subject's age (at least within a range) and because it's easier to come by than a social security or driver's license number, I find knowing a subject's date of birth to be especially useful in differentiating among online records. Birth dates can be found using a variety of online sources, including school and alumni association websites, professional directories, genealogy references, driver's license and voter records, licensure agency databases, newspaper archives, criminal records, Usenet posts and website guest books. One of my favorite resources for birth date data is a free database called **http://www.birthdatabase.com/**.

Birthdatabase.com claims to have over 120 million birth dates online, indexed for free searches by name, but returning home city and zip code, too. Conducting a birthday search on the site is easy, but culling through the results can be challenging, or downright maddening if your subject has a common name. Although the database returns middle initials, the search engine does not permit the use of middle names or initials as search criteria.

Gathering social security and driver's license numbers typically requires use of a commercial database (discussed *infra*), but the cost is nominal, often no more than a dollar.

Search Engines

The web is a library with no official card catalogue and stacks of books piled to the ceiling in no particular order. Maybe that's why we call our Internet software a "browser" and not a "finder." But, don't despair! By now just about everyone knows help is available in the form of free indexing services called search engines. Search engines permit you to search large chunks of online information by keywords or subject areas. Though some might quibble, the best search engine remains **Google.com**, though **YAHOO.com** remains a friendly and popular starting point for Internet research. Others include **MSN.com**, **Ask.com**, **MyWay.com** and the inelegantly named **Dogpile**. A reliable search engine makes an excellent start page for your browser, and the leading providers allow you to customize the start page with your preferred content.

But remember, no search engine is exhaustive—Google covers far less than half of the web, and studies suggest that much of the content indexed by each search engine is unique to that engine--so expect to run some searches across several engines. All the sites listed above are free.

Googlizing

No discussion of search engines would be complete without the incomparable **Google.com**. Google is so good at what it does that cybersleuthers have turned it into a term for running a broad Internet search: "to Googlize." With access to 8+ billion web documents, its data include web pages, images, Word, PDF and PowerPoint documents and newsgroup messages. It's the biggest, it's the best, and it's free. But even Google has limitations: The most effective online skip tracing tools (voter, driver's license, and criminal records, to name a few) aren't indexed by Google but reside on the "hidden" or "deep" web; that is, in online databases that require specific searches or membership.

.

Getting the Goods with Google

Google is so important to cybersleuthing that it's worth the effort to study how to get the most from a Google search. Though most of us simply drop a few keywords into the search box and hope for the best, you'll get the most relevant hits and speed your efforts by learning some of the powerful tweaks available for advanced searching.

Unless you otherwise indicate, Google assumes that all words entered into the search box are conjunctive—it inserts “and” between them. Google doesn’t care about capitalization—it’s case insensitive—but the order in which search terms are entered can affect the results so start with the broadest keywords followed by more narrow ones. Google ignores punctuation and turns a blind eye to a long list of “noise” words so common that it assumes you didn’t intend to search for them. Examples of noise words are “the,” “where” and “how.”

But what about when you don’t want a search term ignored? To be certain that the search result always includes a particular word, precede it by a plus sign (e.g., defective product +toaster). More often, you’ll need to exclude a particular word from search results, so precede the words you don’t want with a minus sign (e.g., corporate fraud –Enron –WorldCom -Tyco). This is a handy way to limit results when one of your search terms has multiple meanings (e.g., crash –computer -movie).

When used with care, one of the very best ways to narrow your search results is by putting target phrases in quotes. When you’re confident that a phrase appears in the result, enclose two or more words of the phrase within quotation marks (e.g., “head trauma” seizures). When searching for information about a person, you’re more likely to find useful hits if you place the person’s name in quotes, but don’t forget that databases may include middle initials or index names in the “last name, first name” manner.

A little known feature of Google is its ability to search synonyms. If you precede a search term by a tilde, Google will search for that term and its synonyms (e.g., ~drug will also search for medicine and pharmaceutical).

If you want to specify alternate search terms, you can separate them by the word “OR,” but be sure that it’s in all capital letters (e.g., “adverse reaction” diazepam OR Valium).

There are many other operators that allow you to narrow your Google search, and the easiest way to use them is to click on the Advanced Search option adjacent to the search box or go to google.com/advanced_search. Here, you’ll be able to fine-tune your search by, inter alia, language, format, date and domain.

In addition to its massive web index, Google offers specialized indices that are help hone in on a search subject. For example, Google Images searches pictures; Google News indexes news stories; Google Book Search explores the full text of countless published works; and Google Scholar explores scholarly literature like peer-reviewed publications and PhD theses. Google Groups indexes over a billion Usenet postings extending back some twenty-five years, and includes many candid remarks and revealing discussions that may prove useful in vetting clients or cross-examination.

Google never ceases to amaze in terms of the little miracles it performs. For example, Google loves numbers. Enter a package tracking ID number as a search and Google recognizes the format and returns information about parcel’s status. You can run a car’s vehicle ID number (VIN), an airplanes FAA registration number (n-number) or a product’s

UPC code. You can even retrieve a patent by entering the patent number. In a pinch, it's also a capable calculator and currency converter.

Phone Directories

Two decades ago, skip tracing entailed poring over dozens of phone books and reverse directories at a big-city public library. Now, the Internet makes it possible to check nearly every phone book in the nation in seconds, at no cost. Sites like **Switchboard.com**, **Lycos People Search** (http://peoplesearch.lycos.com/, formerly WhoWhere.com), **AnyWho.com** and several others link to millions of listed numbers and cross-link to maps, physical addresses, e-mail addresses and a mix of other free and for-fee services. A powerful feature of some online white pages is the ability to reverse search by phone number or address to find the name of the holder. Reverse searching supports skip tracing by identifying neighbors (or former neighbors) of the subject who may know whereabouts.

You can simply access all the major telephone databases via **Craig's Phone Finder** at **www.craigball.com/phone**.

Real Property Records

Counties from coast-to-coast have rapidly made their real property and appraisal district records accessible via the Internet. In addition to identifying assets that may be subject to execution, these records may locate family members or identify a subject's landlord or former landlord (who may be able to furnish a forwarding address). Real property records also offer insight into financial, marital and family relationships. Although no site has emerged as the definitive source for free online real property and appraisal records, two sites are good starting points: **www.netronline.com** and the Property records area at **www.searchsystems.net**.

Genealogy and Death Records

Genealogy databases are fertile sources of skip trace data. Birth, marital, divorce and death records are all found on the major sites. There are dozens of such sites; however, the premier, partially free, genealogy sites are **www.ancestry.com** and its affiliate **www.rootsweb.com**. A third site, **www.Familysearch.com**, is a searchable database of 400 million names maintained by the Mormons. Finally, try **www.legacy.com** to search the obituary records of hundreds of newspapers. When Grandma shuffles off this mortal coil, even the most private person ends up listed as a survivor in the obituary, often with the name of the place they currently reside and the names of their siblings, spouse and children.

Criminal Records

The ultimate source of criminal records, the FBI's database called the **National Crime Information Center,** is off limits to all but law enforcement personnel. It's the closest thing to a nationwide criminal records database as exists, but even this definitive resource doesn't contain complete records for all 50 states. Furthermore, while law enforcement officers have run the occasional search of the NCIC as favors for friends, strict penalties apply for unauthorized access and trafficking in illegally obtained data. As a result, gathering criminal convictions data on a nationwide basis can be tough. Some criminal records are available online without charge. These records are linked at the excellent **Search Systems** site (**www.searchsystems.net/**). Many fee-based criminal records search services have sprung up, including a few operated by law enforcement agencies. Charges for criminal records searches vary widely; one of the best is www.choicepoint.com, an expensive resource geared to lawyers, collection agencies, and other investigative professionals.

The Cousin Bubba Factor

Perhaps you believe you are guarding against an accumulation of personal data about you on the web. You don't give out your social security number or participate in online forums, own a house, or even have a driver's license. But never underestimate the Cousin Bubba factor. You remember your second cousin Bubba, don't you? The one with that unfortunate hygiene problem and the lazy eye? Well Cousin Bubba is now a genealogy buff, seated at his computer putting every detail of your life—along with those of your siblings, wife, and kids—into an Internet family tree database for the entire world to see. You think your mother's maiden name is a big secret? Cousin Bubba makes sure it's not!

Commercial Providers

Literally hundreds of data brokers sell their services online, from law-abiding corporate behemoths like Choicepoint and Experian to fly-by-night outfits on both sides of the law. Data brokerage is not a venue where you necessarily get what you pay for. Some companies charge big bucks for data available online for free, while reputable firms like Accurint, KnowX, Intelius, or USSearch offer their services at very reasonable prices. Choose your suppliers wisely because the law impose criminal penalties upon not only those who perform certain illegal searches but also those who purchase them. Be wary of providers who promise to furnish current bank or brokerage account balances—such information is available for sale, but it almost certainly was acquired in violation of the anti-pretexting provisions of the **Gramm-Leach-Bliley Act**, 15 U.S.C.A. Section 6801 et seq. (2000)

Here's the lowdown on several commercial providers trading online:

Accurint: www.accurint.com (a division of Lexis-Nexis)

What sets Accurint apart is the high quality of its data and its prices, which are just dirt cheap. Accurint can find your subject for a buck and will deliver a comprehensive dossier of addresses, relatives, neighbors and more in seconds, for $8.50. The interface is intuitive and intelligent, and the system allows users to track usage by account or client number and

LexisNexis®
Accurint®
for Legal Professionals

authorize use by others within an account. The owner of the account can set additional user IDs and passwords, as well as program access limits for authorized sub-users. In addition to its focus on skip tracing, UCC filings and phone numbers, Accurint has added drivers' license, court and criminal records. On a scale from one to wow, Accurint is a WOW!

ChoicePoint: www.choicepointonline.com
No private web resource approaches ChoicePoint's data muscle of over seventeen billion public records. ChoicePoint sells to sectors--including the legal profession--willing to pay its prices and jump through the hoops of its registration process. ChoicePoint is not cheap, entailing a monthly subscription fee in addition to hefty search charges, but it's probably the best resource for background personal data and online public records. Let's put it this way: the U.S. Government buys data from ChoicePoint! (Some users report the subscription fee is negotiable, so be sure to ask).

KnowX: www.knowx.com
KnowX might fairly be called "the poor man's ChoicePoint;" (it's owned by them). KnowX sells to anyone and heavily markets its wares through Internet banner ads and strategic partnerships with search engines and portal sites. There's no subscription fee (although you can purchase day- and month-long passes) and search prices range from free to $29.95. Its free "Ultimate People Finder" is hard to beat and works well for skip tracing a name to a locality.

Locate Fast: www.loc8fast.com
Locate Fast is a mix of search-it-yourself resources and assisted search options, largely focused on California data. Prices are modest, ranging from $5.00 for a simple people finder to $20.00 per state for a Wants and Warrants search. One jarring note is its attempt to charge for database services (like the death or licensed pilot indices) that are available without charge everywhere else.

Public Data: www.publicdata.com
This inexpensive database contains records of licensed drivers, sex offenders, voters, vehicle license tags, criminal records (31 states) and voter rolls. It offers motor vehicle and/or drivers' license data for Florida, Idaho, Iowa, Maine, Minnesota, Mississippi, Missouri, Ohio, Texas and Wisconsin. Publicdata.com is a bargain. A month's subscription at $9.95 entitles you to 200 searches; a year of access and 250 searches costs just $25.

USSearch: www.ussearch.com
If you are uncomfortable doing searches yourself, or if your time is better spent elsewhere, USSearch may be the

resource for you. Although you can do the searches on your own using their database, for an added fee, USSearch will do the work and e-mail the results. Standard turnaround time is under 24 hours, but they usually beat that. The "Expert Assisted People Locate" costs about $60 and includes address history, possible aliases, names of relatives and neighbors, bankruptcies, tax liens, real property ownership, and more.

FlatRateInfo: www.flatrateinfo.com:
With annual subscription rates starting at $1,400.00, the service makes sense only for who conduct thousands of searches per year. . FlatRateInfo.com offers unlimited access to credit headers, property ownership, phone numbers, and the like for a flat fee. If you have the budget and the volume, this is a great tool.

TrialSmith: www.trialsmith.com
Exclusively for use by plaintiffs' trial lawyers, TrialSmith puts the full text of over 270,000 depositions and many other resources at your fingertips. Member trial lawyers can search at no charge and purchase information only as needed. Additional services and lower deposition costs are available by subscription. There is nothing else like this out there, and it is an extremely well crafted resource.

Credit Reports
A credit report can be very revealing. Typically, a credit report will include five primary categories of information: personal data, credit history, public records entries, inquiries and credit score. These five categories include information as follows:

<u>Personal Data: (Credit "Header")</u>
Name
Current and previous addresses
Social Security number
Telephone number
Date of birth
Current and previous employers

<u>Credit History</u>:
Lists the status of the subject's credit accounts for the preceding ten years, including:

- Retail credit cards
- Bank loans
- Finance company loans
- Mortgages
- Bank credit cards

The credit history section reveals how the subject has managed his or her finances. Each entry in this section includes:

- Account number
- Creditor's name

- Amount borrowed
- Amount owed
- Credit limit
- Dates when the account was opened, updated, or closed
- Timeliness of payments

Public Records Entries:
A credit report's public records section includes:

- Tax liens
- Bankruptcies
- Court judgments (including child support judgments)

Inquiries:
A credit report's inquiries section includes a listing of all parties who have requested a copy of the subject's credit report. Some may be other than "official" business inquiries, such as screenings for promotional offers and account management inquiries from past creditors.

Credit Score:
Credit scores are one of the primary tools a creditor uses to decide whether or not to make a loan, how much credit to offer and at what rate. Because most credit decisions are made quickly—one might say "hastily"—and a credit score is ostensibly an objective summary of the credit report, it is frequently decisive. Thousands of score models used in the credit industry consider different variables for different types of credit and credit bureaus offer several different scores in their various products.

Experian: **www.experian.com**
Equifax: **www.equifax.com**
TransUnion: **www.transunion.com**

Experian, Equifax, and TransUnion are the big three consumer reporting agencies and control virtually all of the nation's consumer credit data. Because an unfavorable credit report, can wreck havoc on an individual's financial life, these reports were the first electronic data closely regulated by federal legislation. While each credit reporting agency will happily sell you a copy of your own credit report for less than ten dollars, gaining access to their massive database of details about an another's identity and creditworthiness is a more challenging and costly undertaking. **The Fair Credit Reporting Act (FCRA)** affords consumers certain rights designed to promote the accuracy and ensure the privacy of information contained in credit reports. In theory, only a person with a legitimate business need as recognized by the FCRA or one with express permission from the subject can get a copy of another person's credit report. In practice, the lack of any meaningful oversight of the sale of credit data means that almost anyone willing to pay for it can get a copy of your credit report. Sadly, the FCRA is observed mostly in the breach. The big three are not the primary culprits in this regard, as the transgressions are largely confined to rogue data brokers--who are more likely than not customers of the big three.

Public Records: www.searchsystems.net
A broad sweep of public records is freely accessible via a variety of governmental and private databases. You truly never know what you might find. Resources vary from state-to-state but include the following records: court records, judgments and liens, marriage and divorce, birth and death, professional licensure and discipline, motor vehicle and driver's license, incorporations, limited partnerships, registered agents, assumed names, UCC security filings, property tax appraisal, watercraft and airplane ownership, political contributions, voter registration, bankruptcy, probate, personal property and ad valorem taxes, fishing and hunting licensure, building permits, pet registration, military service, outstanding warrant lists, abandoned bank account lists, sex offenders, criminal offense and inmates, and many more.

The most comprehensive free list of such resources is found at **www.searchsystems.net**. It is extraordinarily complete and well worth checking early in the cybersleuthing process. Another stellar site for access to all manner of U.S. Government records is **www.firstgov.gov**, which accesses more than 50 million government documents.

Two free public records resources deserve special mention: **FECInfo.com** contains records of political contributions made to candidates for federal office, at **www.tray.com**. **Landings.com** affords free access to a database of aircraft ownership and those holding pilots' licenses.

Ball's List: www.craigball.com/links
I'd like to believe that no article on cybersleuthing would be complete without some passing mention to my own modest contribution, **Craig Ball's Sampler of Informal Discovery Links**. This eclectic compendium of investigative resources was created to assist lawyers in gathering revealing information on persons, companies and products involved in litigation. I hope it proves useful to the reader as well.

Checklist for Locating People for Free

Though the fee-based resources discussed in the paper are the most expedient, there are effective ways to skip trace without going out-of-pocket. Her are a few suggestions:

1. Run a Google search for the person using several variants of his or her name. Even those with few ties may show up in a chat room exchange, fantasy football league or picture caption. Unique surnames often turn up relatives who may know the target's whereabouts.
2. While you're at Google, be sure to run the search through Google image, Google News and Google Groups.
3. Run a white pages telephone search through switchboard.com, AnyWho.com, Lycos.com or BigFoot.com.
4. If you know the target's e-mail address, run that too.
5. Check to see if you can turn up a birth date and address using Birthdatabase.com
6. Check state licensing records for the target's training or profession. These are easily found using searchsystems.net. Note: *Reportedly, about a third of adult males have hunting or fishing licenses.*
7. Check alumni websites like classmates.com and online dating sites, too. If you know where the target went to school, check the alumni boards and directories at the school's website. If the target had fraternity and sorority affiliations, check those sites as well (www.greekpages.com).
8. If the target has a hobby or likes to participate in sports, browse sites catering to those interests.
9. For those in active military service, try GISearch.com.
10. Check voter registration records.
11. Check real property ownership records for promising counties. Even a former address may lead to a current residence.
12. Run bankruptcy records, judgments and tax liens.
13. Check the genealogy sites like ancestry.com as well as the Social Security Administration's Master Death Index. If you don't find the subject, check for relatives who may have died to pin down possible residences.
14. Check criminal records and sex offender databases.
15. If your target is politically oriented, run their name through the contributor records at FECInfo.com.
16. Check corporate and partnership records.

Appendix A:
Limiting Online Access Not the Answer to Identity Fraud

Identity fraud is the world's fastest growing crime. Although there are no reliable measures of the prevalence or cost of identity fraud, the U.S. General Accounting Office puts the year 2000 domestic loss to MasterCard and Visa alone at one billion dollars. Because dates of birth, social security numbers, drivers' license data and other public and online records have been used in identity fraud, some want to outlaw the release or sale of these identifiers. The problem with this approach is that not only is the responsibility misplaced; worse, the proposed solution simply won't work.

If a door can be opened by slipping a library card against the latch, fault the shoddy lockset, not the library. Responsibility for the increased incidence of identity fraud, and for its prevention, must be laid at the feet of the banks, credit card issuers, brokerage houses, retailers and others who have failed to adopt improved methods of authentication. Our financial security is anything but secure so long as financial institutions rely on flawed authenticators, like "mother's maiden name" or the "last four digits of your Social Security number."

Will limiting access to public records and outlawing sale of personal data solve the identity fraud problem? No, the cows are long gone from that barn and outlawing online public data will only make it harder to collect debts, screen employees and locate witnesses. According to credit information giant Transunion, the leading source of identity fraud is stolen employer records, followed by credit card cloning and mail theft. Instead of buying information from data brokers, identity thieves rifle through our trash ("dumpster diving"), "shoulder surf" behind us in the check-out line and "skim" encoded data from our credit cards at the local cafe.

Automatic teller machines use a mix of hardware (ATM card) and software (PIN) for authentication. Other financial transactions should employ both to guard against fraud. To combat identity theft, regulators should require banks and other financial institutions, retailers and all entities to which we entrust our savings and credit reputation to employ authentication procedures better suited to a wired and impersonal world. Inexpensive biometric devices, password protection and digital keys, to name just a few alternatives, are a quantum leap toward more secure transactions.

Appendix B
Balancing Private Interests and Public Data

A recent study by the Pew Research Center found that two out of three Americans expect to be able to find government information on the Net, and that one of three Internet users expects to be able to locate and gather reliable information about people online. Why, then, are so many who expect to find online public records and personal data about others dismayed to find the same information is available about them? A concerted effort by government to make public records available online has run up against contradictory expectations and a backlash of misdirected legislation.

Public access to government records is a cornerstone of good governance. Anyone who wishes to do so is free to visit the courthouse and pore through the records. The inconvenience and expense of a trip to the hall of records operated, as a practical matter, to restrict access to the press, commercial users and those with a compelling desire justifying the time and expense. The “practical obscurity” of public records afforded the public a false sense of privacy.

As government embraces the efficiencies and openness afforded by online access, practical obscurity gives way to frictionless access to all manner of personal, though not private, information. Open and less-costly governance, along with improved services, come at the expense of our neighbors’ ability to see how much our home is worth for tax purposes, who holds the note on our car and perhaps even the grounds plead by our ex in that messy divorce. Though potentially embarrassing and subject to misuse, such personal public data has always been available; but, the ease with which it can now be downloaded and aggregated has triggered efforts to restrict access. Security concerns following the tragedies of 9/11 act as a tailwind for such initiatives, at the expense of open government and personal freedom.

Often, notions of privacy are put forward as a surrogate for what people really want: *crime control*. To guard against identity fraud, some seek to characterize identifiers like Social Security or drivers’ license numbers as “private” when they’re not. Instead of trying in vain to suppress access to such information, it would be wiser to blunt their usefulness in criminal activity. Knowing someone’s Social Security number shouldn’t make it easier to access their bank account or secure a credit card in their name.

We live in an information economy. Personal information about us is a commodity that has long been aggregated, analyzed, traded and exploited. Mostly, we benefit from this activity when it engenders lower prices and targeted advertising. When abuses occur, there are a host of legal protections already in place supporting prosecution and compensation. Though the United States has no omnibus legislation covering private use and collection of personal information, a patchwork of laws regulates different types of information. There are statutes covering consumer credit, educational records, videotape rentals, cable TV viewing, electronic communications, motor vehicle records, drivers’ license records and web surfing by minors. In addition to possible violation of laws prohibiting eavesdropping devices, publicizing private matters, publicizing in a false light, or appropriating a person's name or likeness for commercial purposes, cybersleuthers can run afoul of state law and federal statutes, new and old, chief among them:

The Fair Credit Reporting Act (FCRA) – Limiting access to credit information, including the locator data contained in so-called “credit headers.” The FCRA establishes a narrow range of permissible purposes for which such information can be obtained and used.

Gramm-Leach-Bliley Act of 1999 (GLB): Regulating the release and sharing of customer data by financial institutions and prohibiting the use of pretext methods (i.e., misdirection) to gain access to financial data. For most consumers, GLB was an incomprehensible blizzard of densely-worded notices accompanied by no discernable benefit.

The Driver's Privacy Protection Act (DPPA): Although riddled with exceptions, the DPPA governs public access to state motor vehicle registration records and driver's license records, limits how recipients of such records may share them and requires the state agency to tell the person whose information is being requested about the request and secure their permission before sharing the information.

Perhaps one lesson of September 11 is that, where privacy is concerned, rights are not absolute. We see trade offs between privacy and national security, privacy and market efficiency, privacy and convenience and privacy and societal interaction. But in balancing private interests and public data, we shouldn’t let the bogeyman of criminal abuse scare away the real and significant benefits that flow from online access.

CRAIG BALL

Trial Lawyer & Technologist
Computer Forensic Examiner

3402 Cedar Grove
Montgomery, Texas 77356
E-mail: craig@ball.net
Web: craigball.com
Lab: 936-582-5040
Cell: 713-320-6066
Fax: 936-582-4234
Home: 936-448-4321

Craig Ball is a Board Certified trial lawyer and computer expert. He's dedicated his twenty-four year career to teaching the bench and bar about forensic technology and trial tactics. Craig now limits his work exclusively to serving as a court-appointed special master and consultant in electronic evidence, as well as publishing and lecturing on computer forensics, emerging technologies, digital persuasion and electronic discovery. Craig Ball has extensive experience in the use of computer forensics to track and prove the theft of trade secrets and intellectual property. Craig's monthly e-discovery column, "Ball in Your Court," appears in Law Technology News. While Chair of the State Bar of Texas' Technology Advisory Committee, Craig Ball created the MYTexasBar web portal used by over 47,000 Texas lawyers. Named as one of the Best Lawyers in America and a Texas Superlawyer, Craig is a recipient of the Presidents' Award, the State Bar of Texas' most esteemed recognition of service to the profession.

EDUCATION

Rice University (B.A., triple major, 1979); University of Texas (J.D., with honors, 1982); Oregon State University (Computer Forensics certification, 2003); EnCase Intermediate Reporting and Analysis Course (Guidance Software 2004); WinHex Forensics Certification Course (X-Ways Software Technology AG 2005).

SELECTED PROFESSIONAL ACTIVITIES

Law Offices of Craig D. Ball, P.C.; Licensed in Texas since 1982.
Board Certified in Personal Injury Trial Law by the Texas Board of Legal Specialization
Certified Computer Forensic Examiner, Oregon State University and NTI
Special Master, Electronic Discovery, Federal and Harris County (Texas) District Courts
Instructor in Computer Forensics, United States Department of Justice and National Cybercrime Summit
Member, Editorial Advisory Board, Law Technology News (American Lawyer Media)
Special Prosecutor, Texas Commission for Lawyer Discipline, 1995-96
Council Member, Computer and Technology Section of the State Bar of Texas, 2003-
Chairman: Technology Advisory Committee, State Bar of Texas, 2000-02
President, Houston Trial Lawyers Association (2000-01); President, Houston Trial Lawyers Foundation (2001-02)
Director, Texas Trial Lawyers Association (1995-2003); Chairman, Technology Task Force (1995-97)
Member, High Technology Crime Investigation Association and International Information Systems Forensics Association
Member, Institute of Computer Forensic Professionals and FBI Infragard
Member, Texas State Bar College
Member, Continuing Legal Education Comm., 2000-06, Civil Pattern Jury Charge Comm., 1983-94,State Bar of Texas
Life Fellow, Texas and Houston Bar Foundations
CLE Course Director: E-Discovery A to Z (NY, Chicago, SF, Boston, Washington, D.C. and Minneapolis) 2004; Electronic Evidence and Discovery 2004, 2005, 2006; Advanced Evidence and Discovery Course 2003; 2002; Enron—The Legal Issues, 2002; Internet and Computers for Lawyers, 2001-02; Advanced Personal Injury Law Course, 1999, 2000; Preparing, Trying and Settling Auto Collision Cases, 1998.
Member, SBOT President's "Vision Council" on Technology, 1999-2000; Strategic Planning Committee Liaison, 2001-02; Corporate Counsel Task Force 2001-02
Admitted to practice U.S. Court of Appeals, Fifth Circuit; U.S.D.C., Southern, Northern and Western Districts of Texas.

ACADEMIC APPOINTMENTS AND HONORS

The March 2002 CLE program planned by Mr. Ball and Richard Orsinger entitled, “Enron—The Legal Issues” received the Best CLE of 2002 award from the Association for Legal Education
Recipient, State Bar of Texas Presidents’ Award (bar’s highest honor), 2001
Faculty, Texas College of Trial Advocacy, 1992 and 1993
Adjunct Professor, South Texas College of Law, 1983-88
Listed in “Best Lawyers in America” and Selected as a “Texas Super Lawyer,” 2003 and 2004
Rated AV by Martindale-Hubbell

LAW RELATED PUBLICATIONS AND PRESENTATIONS

Craig Ball is a prolific contributor to continuing legal and professional education programs throughout the United States., having delivered over 400 presentations and papers. Craig’s articles on forensic technology and electronic discovery frequently appear in the national media, including in American Bar Association, ATLA and American Lawyer Media print and online publications. He also writes a monthly column on computer forensics and e-discovery for Law Technology News called "Ball in your Court." The presentation, "Craig Ball on PowerPoint," is consistently the top rated educational program at the ABA TechShow.