Protecting Your Personal Privacy

A Self-Help Guide for Judges and Their Families

Published by The Chicago Bar Association and The John Marshall Law School Center for Information Technology and Privacy Law

October, 2006

Today more than ever, Americans are painfully aware of the reality of increased violence and threats against the federal and state court judiciary. These threats undermine our democratic government and shake the very underpinnings of America's system of justice. If our society is to remain free, these threats cannot be tolerated and must be effectively addressed by the state and federal government and, of course, by the dedicated men and women who serve in our third branch of government.

In an effort to reduce the security and privacy risks to judges stemming from the availability of their personal information, The Chicago Bar Association in conjunction with members from our state and federal judiciary established the Privacy Task Force to study and address the myriad of complex privacy issues surrounding the need for greater judicial security. The Task Force was comprised of state and federal court judges, federal, state and local law enforcement officials, constitutional lawyers, academicians, and leading lawyers from the community.

The Task Force conducted a comprehensive review of state and federal privacy laws, including statewide legislative initiatives designed to enhance judicial security. The Task Force also consulted with court administrators, law enforcement and government officials, state and federal court judges, and mental health and security experts from within and outside of Illinois.

The Task Force concluded that invariably, the information technology explosion will continue to draw, catalogue and profile, in ever more sophisticated ways, personal lifestyle information and habits of all Americans – including judges. How, where and when it is permissible to use this information presents challenging constitutional issues which continue to evolve in our courts. However, the speed and sophistication with which this information is being obtained and the sources from which personal data is being gathered is remarkably broad. Cell phones, electronic transportation passes, e-mail, wireless computers, personal internet messaging devices, voter registration records, and credit card purchases are only a few of the extraordinarily wide range of sources from which personal information is both legally and illegally being drawn. Notwithstanding our personal preference, much of this information is obtained because people are unaware that certain methods of electronic communication are insecure. They are also unaware of options and alternatives to protect their privacy. Once this personal information finds its way into a databank its distribution via the internet can be limitless and frightening.

While federal and state legislative initiatives have helped somewhat, much more needs to be done to protect the privacy of state and federal court judges. Trying to limit or restrict the ever growing sources of personal information about judges on the Internet is extremely difficult but there are things that judges can do to help protect their privacy. This guide was developed by the Privacy Task Force to make judges aware of the options they have to narrow and possibly eliminate the sources from which their personal information is publicly available.

We are grateful to the dedicated men and women who served on the Privacy Task Force. We welcome your comments and suggestions for improving the Guide.

Sincerely,

Joy V. Cunningham
Co-Chair

Collins T. Fitzpatrick
Co-Chair

The Chicago Bar Association Privacy Task Force

Table of Contents

The CBA's Privacy Task Force is grateful to The John Marshall Law School Center for Information Technology and Privacy Law and Professor Leslie Ann Reis for their research and assistance in preparing this manual.

"I believe that the Internet is a brave new world in the matter of judicial security."
–Testimony of Joan H. Lefkow, United States District Judge, before the Judiciary Committee of the United States Senate (May 18, 2005).

Introduction

Your personal information may be no farther away than a mouse-click...

Your name, locations of your home and workplace, your phone number and email address, details of your family members, your political leanings and many more pieces of information are available through a wide array of public and private sources. But, this is nothing new. Some personal information about you has always been accessible by others in one form or another. In the past, when information such as that contained in public records was maintained in paper files, it was difficult to access. However, information technologies, including the Internet, have changed the way data is collected, stored, used, manipulated and distributed -- making more information more accessible to more people than ever before.

There are no comprehensive laws to protect your personal information. However, there are ways to keep information about you and your family from becoming generally known. As you become aware of the potential privacy risks associated with even the most common activities of daily life, you will be able to make reasoned choices affecting the availability of your personal information. The purpose of this pamphlet is to provide the tools to help you take control over your personal information and protect your informational privacy.

Please note that protecting your privacy is a continuing process because data about you is constantly being collected and distributed.

Steps You Can Take To Limit The Amount Of Your Personal Information That's Available To Others

Know the Landscape

You can reduce the amount of your information that is available to others. The first step is to educate yourself about how your personal information gets into the public domain, and what information about you is already in "the stream" of publicly accessible or available information.

Personal information gets into the public domain in a number of ways including public records, public information, operation of law, non-public information exchanged through contractual relationships and information you volunteer to others.

Public Record Information

Public record information is collected and maintained by various government entities. Real estate transactions, business ownership, court filings, marriage and death certificates are a few of the types of data that are deemed public records. By definition and long-standing tradition, public records are open to the public for inspection. The policy underlying such openness is to promote transparency and accountability of government operations and to ensure the fair and unbiased application of law.

Public record information may be legally gathered by private entities, cross referenced, mined for data and sold to third parties. There are few, if any, restrictions on the use or redistribution of the information contained in public records. Once information is put into the stream via public record, it's out there and there's no way to get it back. Be aware that a great deal of public record information about you has already been accessed and distributed for commercial and noncommercial purposes many times over. You cannot reclaim that information, but you can be pro-active going forward.

The best way to keep your information private is to limit the information you put into the public record and therefore into the **public domain** in the first place. For example, in some states, you can avoid putting title to your residential real estate in your own name through the use of a land trust (see explanation on page 6).

Personally Identifiable Information ("PII")

PII is information that can, in and of itself, identify you as an individual. It is any specific fact that could be used to uniquely, contact or locate a person.

PII includes, but is not limited to: your full name (especially if it is not a common name), telephone number, street address, driver's license number, credit card numbers, passport numbers, bank account information, employee identification cards, biometric information (fingerprints, DNA, etc.) and social security number.

PII coupled with other personal information, such as buying habits, can be used to predict future consumer behavior and has become an increasingly valuable commodity that supports a multi-billion dollar industry dedicated to the creation, manipulation, and distribution of personal information. "Information brokers" rely heavily upon data obtained from public records as well as other sources, to create massive databases, customer lists and other products sold primarily for marketing purposes.

Publicly Available Information

Publicly available information includes personal information about you that is accessible to the general public from a number of non-governmental sources including newspaper articles, telephone directories and websites (such as your employer's, professional organization's or alumni association's websites). In some instances, you can take steps to limit the amount of your personal information that is publicly accessible. Examples include obtaining an unlisted telephone number and not listing your home address or family details in professional or alumni directories. Note, however, that some publicly available information originates from other records or activities over which you have little control (such as public records and participation in high profile, newsworthy events). As judges are public figures, some press coverage is inevitable.

Operation of Law

Some personal information is put into the public domain by operation of law. For example, you may be compelled to provide personal information that will be made public in the course of obtaining a professional license, running for office or participating as an officer of a non-profit organization (certain IRS forms that may include your personal information, such as form 990 – Return of Organization Exempt from Income Tax, are considered public records).

Voluntary Information

Much of the personally identifiable information about you is "out there" because you put it there voluntarily. Both public and private entities collect consumer transaction information that may find its way into a **Data Broker's** database. Some personal information is collected when you fill out surveys or warranty cards, apply for credit, open consumer accounts, or use retail store discount cards. Once you volunteer your personal information, especially to private sector entities for commercial purposes, you likely lose control over its future use. However, there are a number of steps you can take to limit the amount of voluntary information that gets put into the stream. For example, do not provide your home address or home phone number in connection with any retail purchase and have mail order purchases delivered to your office or post office box address. There are also ways you can limit the distribution and redistribution of information that's already out there. In some cases, you may request that companies not share your personal information with others (see Opt-out! on page 5).

Loyalty or Reward Cards

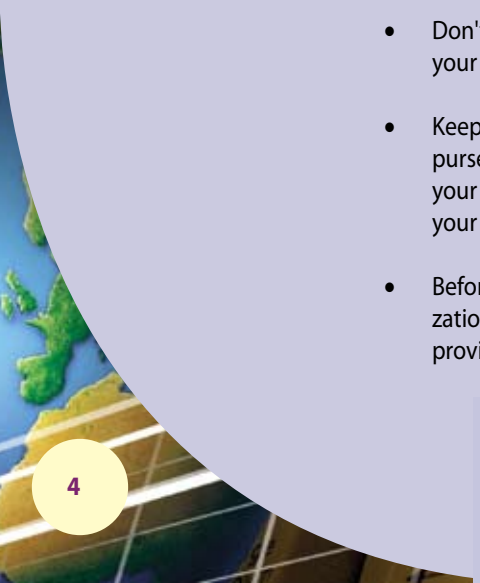
Frequent shopper or reward programs offered by many retailers often provide shoppers with discounted prices. However, in exchange for discounts, the card holder's purchases are tracked. Purchase information, together with personally identifiable information, is maintained in a database. This information can be mined and used for marketing purposes and potentially shared with others.

Some retailers permit shoppers to register for loyalty programs as anonymous users. Certain discounts and benefits, such as check cashing privileges, available to loyalty card holders may not be available to anonymous users.

In addition, retailers using product scanning equipment can also track and personally identify your purchases if you pay using a check or credit card. If you want to ensure that your purchases are anonymous, use cash and do not participate in loyalty programs.

General Tips

- Avoid completing product registration cards, warranty cards, consumer surveys and other promotions that require you to submit personal information.
- Avoid entering online contests. In order to enter these contests you need to provide personal information that may be used for marketing or other purposes. Although you may actually receive a prize, it is generally not worth the damage that may result from the use or misuse of your personal information.
- Never give out personal information on the phone, through the mail, or over the Internet unless you've initiated the contact. Your Internet service provider, bank, creditors, and other service providers will not contact you asking for personal information. If someone contacts you purporting to be from one of these entities, it is likely that the person is an impostor.
- When you must provide a physical or mailing address, use your work address instead of your home address whenever possible. Consider obtaining a post office box and use that address as a mailing address.
- Remove your name, home address and telephone number from many mailing and telephone lists through the Direct Marketing Association's Mail and Telephone Preference Service by visiting **www.dmaconsumergs.org/offemaillist.html.**
- Memorize all of your passwords. Don't record them on anything you keep in your wallet.
- Don't carry your social security card, social security number, birth certificate, passport or extra credit cards in your wallet or purse unless absolutely necessary.
- Keep a list (or photocopy) of all documents containing personal information that you carry in your wallet or purse. Keep that list in a safe location. Be sure to include the telephone numbers of customer service for all of your credit card providers. This will ensure that you can promptly report and cancel accounts in the event that your wallet or purse is stolen.
- Before providing your personal information or biographical information to alumni associations or other organizations to which you belong, make yourself aware of their information sharing and disclosure practices. Avoid providing any information about spouses, significant others and children to any organization.



Opt-out! A Powerful Weapon

In some cases, you can request that your personal information not be shared with others.

The term "opt-out" is often used in connection with information sharing practices or marketing programs and assumes inclusion -- i.e., by your silence, you give permission for your information to be shared with others, or to receive advertisements for services UNLESS you explicitly deny such permission.

Many entities that collect personal information from you provide some method of opting out of their information sharing practices. Some companies provide toll-free telephone numbers or websites where you can opt-out. In fact, some are required by law to give you this option. Each entity establishes its own procedures. There is no universal opt-out. It is up to you to pro-actively look for and take advantage of opt-out opportunities. This is particularly important when it comes to your financial information.

Financial institutions that collect and share your personal information with others have a legal duty to notify you of their information sharing practices and provide a way for you to opt-out of any third-party affiliate disclosure. You also have the right to opt-out of affiliate information sharing regarding how credit-worthy you are, even though financial institutions can still disclose information about your check writing and credit card history, the deposits and withdrawals you make at your bank, which charities and religious organization you support, and which political candidate you support. Some financial institutions have over 1,000 affiliates and they would all be privy to this information. If you fail to exercise these opt-out provisions, aside from your account numbers, balances and security pin codes, financial institutions can disclose almost everything else in their files they have collected about you.

Now that banks can affiliate with insurance companies and brokerage firms to create one corporate entity providing a warehouse of financial services, your financial information could be merged into a larger database and accessed by more people. It is important to know that your information is constantly being collected by one entity and sold to another, just like a commodity. Once your information is disclosed, it is practically impossible to retrieve. By exercising the financial opt-out features, you can limit any future disclosures of your personal information.

- Avoid using your professional title on anything.
- Secure all documents that contain personal information whenever you have guests, employ outside help, or have service work done on or in your home.
- Shred all documents you throw away which may contain personally identifiable information, such as charge receipts, credit card applications or offers, insurance forms, physician statements, checks, bank statements, etc. Make sure that your garbage does *not* contain any other personal information. Keep trash in a safe/secure location until trash is scheduled to be collected.

Land Trusts

Real estate ownership and transaction information is a matter of public record. If you own your residence and it is titled in your name, any one can readily find out where you live. This information is available at county clerk's offices and, increasingly, online. Moreover, this information is compiled by commercial data brokers and others to be resold for a variety of purposes.

However, there are ways for you to de-identify your real estate holdings. One of the most effective, and perhaps least used privacy protective devices is the land trust.

Available in some states, a land trust is an instrument that may be used to protect information regarding property ownership and may also provide other legal advantages as well. While a land trust does not provide absolute protection against public disclosure of your personal information, it will serve as a barrier to obscure property ownership from public view. Simply, a land trust will allow you to remove your name from the public record by transferring title of your real property to a trustee to hold for the benefit of a beneficiary i.e., you, the actual owner. In most instances, you can retain the benefits of ownership (including deductibility of real estate taxes and mortgage interest).

In addition to keeping ownership details private, the benefits of a land trust include: protecting information regarding your net worth and wealth, suppressing sales price information, avoiding probate and complications of a will, simplifying management by multiple owners, keeping paperwork and legal issues confidential, and allowing the sale of property despite liens and judgments against your name.

While one can buy property and deed it to a trust later, the best way to fully realize the privacy protective benefits of a land trust is to have a seller deed the property directly into a trust.

State laws and statutes applicable to land trusts vary. Consider utilizing land trusts in states that allow some form of it.

At Home

- Whenever possible use your work address instead of your home address for postal correspondence.
- Disclose your home address only to trusted third parties or when required by law.
- Put your house or other owned real estate in a trust or an LLC. This shelters your home address from being associated with your name.
- Do not register your address with the United States Postal Service as your "permanent" address. Even if that is the case, by checking "permanent address" your address goes into a different database and notifies a number of companies about this change (see postal information on page 12).
- Use a P.O. Box or business address on personal checks.

Your Home When You're Not At Home

- Put a hold on your newspaper subscriptions while traveling away from home.
- Do not provide specific details (travel dates for example) on personal email or voicemail "away messages."

On The Road

Your Vehicle

- Technologies used to facilitate services like "On-star" or "I-Pass" may be used to track your vehicle's location. Familiarize yourself with the information sharing practices of the companies that provide these services and opt-out whenever possible.
- Remove any items containing your personal information from your car's glove box or from under the seats.

Traveling

- Make travel reservations in advance over the telephone, rather than at the airport.
- Pick up your tickets prior to the date of departure, and get advance seat assignments whenever possible.
- Never use your official title when making reservations.
- Keep your travel plans confidential within the family. Instruct family members to do so as well.
- When arriving at airports, check your luggage as soon as possible, and remain within the security area as much as possible.
- Travel using a Tourist Passport. Leave any official identification at home.
- Never use your official title on luggage tags. If possible, use a phone number or cell phone number, rather than a home address, on luggage tags.
- When traveling overseas, provide your local U.S. Marshal with your itinerary, airline reservations, hotel and other accommodations, and any contact information of places where you can be located.
- Technologies used in mass transit account-based or pre-paid **smart cards** may be used to track your location, movements, or travel patterns through the transit system. Familiarize yourself with the privacy policies of the transit authority before using mass transit "smart cards."

Motor Vehicle Information

Motor vehicle records often contain personal and personally identifiable information such as your name, home address, Social Security number and medical information. Federal law prevents any state department of motor vehicle (DMV) from disclosing personal information about any individual obtained by the department in connection with a motor vehicle record, except for specific statutorily defined purposes.

The Drivers Privacy Protection Act of 1994 (DPPA) forbids state DMV's from distributing personal information to marketers without your consent. However, the Act does permit disclosure of personal information to government agencies, law enforcement officials, courts, private investigators, researchers, insurance underwriters and other businesses. Check with your state DMV to learn more.

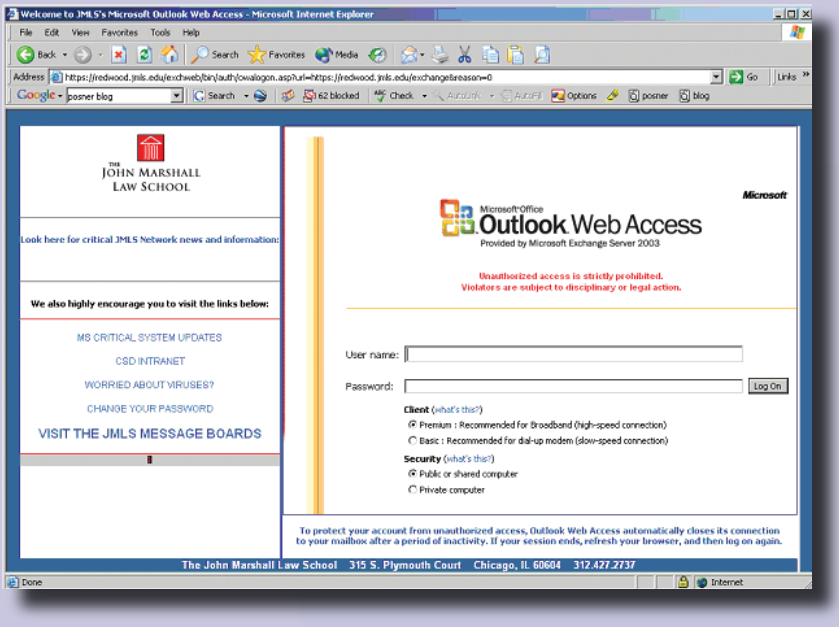
Commercial data brokers or investigative services, such as Docusearch and DMV.org, may provide access to motor vehicle information for DPPA permitted purposes for a fee. These companies require requestors to affirm that they are obtaining information for a lawful purpose. However, disreputable requesters have been known to skirt the requirements and fraudulently obtain information.

In The Digital Environment

Computer And Internet Use

- Use a **firewall** and **anti-virus protection** on your computer, especially if you have high-speed Internet, or any other kind of "always on" connection to the Internet.

- Regularly update your anti-virus protection.



- Act immediately if your computer is infected with a virus.

- Back up all important files.

- Turn off or remove software features that you do not use. For example, disable **remote access** or instant messaging when not in use.

- Be sure to download system updates for your computer as soon as they become available. Do this manually as opposed to automatically.

- Make sure to secure any wireless networks you may use at home. Most store-bought **wireless routers** are not secure by default. You must enable the security functions on your own. If you are unsure of how to do this after reading the instructions provided, call the manufacturer's technical support line.

- Avoid storing sensitive personal information on laptops, cell phones or **personal digital assistants** (PDAs).

- Choose "strong" passwords for your computers, cell phones and PDA's. "Strong" passwords will contain combinations of letters (both upper- and lower-case), numbers and symbols and should be at least eight characters long. Don't use names of relativeor pets, or birthdays, anniversaries, or other easily-guessed dates or numbers as passwords.

- Avoid using automatic log-on features that save your username and password on your computer.

- Make sure you log off your computer when you are done using it.

- Never throw away your old computers without permanently erasing or "wiping" the hard drive. This can be done with a wipe **utility program**. Information that is merely deleted or moved to the recycle bin may still be readable. Wipe utility programs make your old files unrecoverable. An alternative is to remove and physically destroy the hard drive – for example, by drilling a hole through it.

- Read website privacy policies. They should answer questions about the accuracy, security and control of any personal information the website collects, as well as how it will be used, and who will have access to it.

- Whenever you submit personal information online, look for the "lock" icon on the status bar of your browser. The lock icon indicates that the online communication is secure. If the lock icon is not present, the information you are sending is not **encrypted**, and can be intercepted by a third party.

Online Purchases

- Avoid ordering any unsolicited products and services online.
- Avoid purchasing products online from businesses with which you are unfamiliar.
- Avoid using online **wallet services**, which store your credit card and other financial information. While they may make online shopping easier, they are also a security risk.
- Do not allow your browser or any online retailers to store your login information. Always log in manually.
- Do not use your real name, initials or a combination thereof as your username for online retailer accounts.
- Do not access websites from links embedded in unsolicited emails you receive from senders you do not know or from commercial entities such as banks, credit card companies or online retailers. Instead, navigate to the website manually by using a bookmark or entering the URL into the navigation bar of your browser. By doing so, you will likely prevent yourself from falling victim to a common identity scam known as **phishing**.
- Fully research any online investing services before using them. If you must use them, only use those you have heard of before, or that have been referred to you by a friend or colleague.

Email

- Assume that your email is not secure and that email you send can be intercepted, accessed and read by people other than the intended recipient.
- Email you send and receive may be held in storage for a period of time after you delete it.
- Do not send personal information via email unless absolutely necessary.
- Use spam filtering software.
- Use and regularly update anti-spyware and anti-virus software.
- Do not open links or download attachments from anyone you don't know.
- Do not provide login information to businesses that request it via email.
- Do not complete unsolicited email surveys or forms (especially those that request personal information) unless you know the sender.
- Be suspicious of emails marked "important" or "urgent" unless you know and trust the sender.
- Disable the "preview" window of your email system. Using email preview functions can allow you to see what an email message refers to. However, these functions can pose a security risk. They may automatically launch applications or open email born computer viruses without your knowledge.
- If the email address issued by your Internet service provider contains your name, consider using a different address for your primary email account. You can obtain a free email account from many providers, including Google (www.gmail.com), Yahoo (www.yahoo.com), and MSN (www.hotmail.com).
- When sending email to multiple recipients, insert addresses in the blind carbon copy (BCC) box instead of the "TO" or "CC" boxes.

Exposing Yourself and Your Thoughts to the Entire World

www.insertyournamehere.us

A website is a collection of content or pages common to a particular **domain name** or on the **World Wide Web** on the Internet. Companies, organizations, government entities (including courts) as well as indidviduals operate websites to provide information and services to the public. Not only is the content or information posted on a website generally publicly available, but so is information relating to the ownership of the site. Thus, if you own a personal website, your ownership information (including your name, physical address, email address and phone number) is available to the public.

Domain names are registered through many different commercial companies ("registrars"). While registrars are required to collect, maintain and make available actual ownership information, it is possible to register a domain in the name of a third party using a registrar's "proxy registration" service for a nominal additional fee. These services can be used for most domain names, although the U.S. Government has prohibited their use for domain names ending in ".us". Ask your registrar for further details.

To blog or not to blog

The term **blog** is a contraction of web log. It refers to a type of website where individuals publish or post entries in chronological order often in the form of journals, diaries, or commentaries. Blogs can be found on individuals' personal websites or on a variety of social networking sites such as Myspace, Facebook, and Xanga. A blog may contain text, pictures, audio or video clips, and links to other blogs or websites. Blog entries are generally available to the public and you should assume that anything you publishing on your blog is published to the entire world. Information published on your blog may be used to identify and locate you. While many bloggers want to be identified with their postings, it is possible to blog anonymously. There are many online resources that provide information about safe blogging, www.eff.org/Privacy/Anonymity/blog-anonymously.php, is one example.

Personal Websites And Blogging

- Avoid posting any information on your website or blog that can be used to identify or locate you. This includes your real name (use a pseudonym if desired), title, home and work address, descriptions of daily travels or activities, and photographs that show identifiable locations.
- Register domain names through a third party if possible.
- Blog anonymously.
- Remember that information posted on personal websites and blogs is available to the entire world. Moreover, even after you remove information from a website, it may continue to be available in archive copies elsewhere on the web. Thus, use your best judgment when posting personal information.

On The Phone

- Whenever possible use your work phone number instead of a home or cellular phone number as a main contact number.
- If you are worried that your phone number will be disclosed by Caller ID, you can request complete call blocking (per line blocking) on your phone. A less restrictive option is selective call blocking (per call blocking) that blocks your number for that particular call.
- Have a "non-published" or "non-listed" residential telephone number. By not publishing your number with directory assistance or the phone book, you prevent cross-referencing of your address with your phone number. You can also unlist your name, address and phone number from the phone book, and just make it available through directory assistance and reverse directory assistance.
- Whenever you call a "toll-free" number (such as 800, 866, 877, 888, and 900 numbers), your phone number will be logged and possibly sold to marketers for mail and phone solicitations.
- To limit telemarketing calls, sign up with the Do Not Call registry and list all home phone numbers, fax and pager numbers, as well as cell phone numbers by visiting **www.donotcal.gov,** or call 1-888-382-1222. To see how the national Do Not Call registry interacts with your state's registry, visit **www.ftc.gov/bcp/conline/edcams/donotcall/statelist.html.** Be aware and cautious of the ways (some of which are listed above) in which you might unwittingly remove yourself from that list.

Privacy Implications of Cellular Phones, Personal Digital Assistants and Wireless Communication Devices

Cell phones have replaced landlines in many households today, partially because they have become a convenient and affordable way for you to stay connected to the world. PDA devices allow you to carry around a mini-computer to send email, download news, research areas of interest, and read documents and file attachments. When PDAs are synchronized with your computer, both devices are put at risk for viruses. Pagers, Bluetooth and other wireless devices also open your phone up for signal interception by a third party. By 2006, all cell phones will contain GPS satellite location-tracking chips for 911 emergency purposes, thus creating a real-time record of where you and your cell phone are at all times.

Digital cell phones and digital cordless phones are better than analog wireless phones to prevent eavesdropping. Even so, you should use a landline when disclosing your credit card number and expiration date or other sensitive personal information. Cordless phones with digital security codes that randomly assign a new digital code when the handset is returned to the cradle provide greater privacy protection. These phones reduce the risk of interception and prevent neighbors with similar phones from inadvertently make calls using your phone number. Speakerphones and baby monitors also pose security risks because they emit radio signals that can be captured by a scanner.

- **Turn off these devices when not in use.**
- **Use password protection for cell phones and PDAs.**
- **Limit the amount of personal and personally identifiable information kept on your cell phone and PDA.**
- **Exercise care when downloading data onto your cell phone or PDA. Only download data from sources you know and trust.**

- A few cell phone carriers currently provide an opt-in wireless 411 directory. If you do not want your cell phone number published, do not opt-in for this service.
- Never give your phone number or zip code to a cashier when checking out at a department store or grocery store.
- You can obtain an inexpensive or even free telephone number for receiving voicemail messages from various providers including K7 (www.k7.net), and use this number whenever you are required to provide a telephone number.

In The Mail

- Deposit outgoing mail in post office collection boxes or at the post office. Install a locked mailbox at your residence to deter theft of your incoming mail.
- Remove mail from your mailbox promptly.
- If you will be away from home, call the U.S. Postal Service (1-800-275-8777) and ask for a vacation hold on your mail.
- Do not fill out and return warranty cards or customer surveys. Warranties are valid without returning the cards. Companies can and will sell customer information obtained via these means. Increased junk mail is often a result.
- Shred all junk mail. Not only does it confirm your address, some of it contains forms that can be used for identity theft. This is especially true for pre-approved credit card applications.

On The Money

Your Financial, Credit And Customer Information

- Opt out of pre-approved credit card offerings by calling 1-888-5-OPTOUT or visiting **www.optoutprescreen.com.** Note that the three major credit bureaus use the same toll-free number to let consumers choose not to receive pre-screened credit offers.
- Tell the three major credit bureaus that you do not want personal information about you shared for marketing purposes. To opt out, you must contact each company separately by mail:

Equifax, Inc.
Options
P.O. Box 740123
Atlanta, GA 30374-0123

Experian
Consumer Opt-Out
701 Experian Parkway
Allen, TX 75013

TransUnion
Marketing List Opt-Out
P.O. Box 97328
Jackson, MS 39288-7328

- Pay attention to billing cycles. Follow up with creditors if your bills do not arrive on time.
- Review your bills and statements for unauthorized use. Look for small dollar amounts, as well as large purchases.
- Cancel all unused credit cards and accounts.
- Whenever possible, use a credit card instead of a debit card for online purchases. Legal protections for fraudulent use of credit cards are much broader than for debit cards.

The Post Office and Personal Information

The United States Postal Service (USPS) collects personal information about you when you visit its website, obtain information or conduct a transaction. It may also obtain information about you from other, commercial sources. However, the USPS will not sell, rent, or divulge this information to outside marketers without your consent, except to respond to your inquiries or facilitate your requests and transactions. It may market other USPS products and services to you with your consent.

Change of Address Information – a hot commodity

Your mailing address or change of address information is not a matter of public record and is not available to the general public through the USPS. The USPS will not disclose address information to you about a friend or family member who has moved. However, the USPS can and does distribute information it obtains when a customer submits a permanent change of address request. Through the National Change of Address Service (NCOA), the USPS can release your new address to anyone who subscribes to the service and has your name and old address. Subscribers include direct marketers, credit bureaus, and other businesses.

The NCOA database includes only information submitted through permanent change of address requests. You can avoid distribution of your change of address information through the NCOA service by making a "temporary" change of address request instead of a permanent one. A temporary request enables you to have your mail forwarded to a new address for up to one year. To ensure that you will continue to receive important mail beyond the temporary forwarding term, you should also directly notify your utilities, bank, and creditors of your new address.

- Follow the opt-out procedures provided by your bank, credit card companies, insurance companies, and investment firms to limit the sale or sharing of your financial information.
- When ordering new checks, pick them up at the bank. Don't have them mailed to your home. If you have a post office box, use that address on your checks rather than your home address so thieves will not know where you live.
- Always take credit card receipts with you. Never toss them in a public trash container. When shopping, put receipts in your wallet rather than in the shopping bag.
- Shield your hand when using a bank ATM machine or making long distance phone calls with your phone card. **Shoulder surfers** may be nearby with binoculars or video camera.
- Ask your financial institutions to add extra security protection to your account. Most will allow you to use an additional code or password (a number or word) when accessing your account. Do not use your mother's maiden name, SSN, or date or birth, as these are easily obtained by identity thieves.
- Review your credit report at least once each year. Be sure all information contained in it is accurate. Correct any erroneous information. You can obtain one free report each year by calling 1-877-322-8228 or visiting **www.annualcreditreport.com**. Note that this is the only authorized online source for you to get a free credit report under federal law. Some other sites claim to offer "free" credit reports, but may charge you for another product if you accept a "free" report.

Social Security Numbers (SSN)

The Social Security Number was created in 1936. The federal government originally intended that the SSN be used only to facilitate Social Security programs. However, over the years, the SSN became a de facto national identifier. Today, the SSN is the key to your credit and banking accounts and is the prime target of criminals. You are required by law to provide your SSN to certain government agencies (examples include the IRS, welfare offices and state departments of motor vehicles). Other agencies may request your SSN, however, you are not compelled to provide it. If any agency requests your SSN, you may ask to see the Privacy Act notice. This will tell you if your SSN is required by law, what will be done with it, and what happens if you refuse to provide it.

In most cases, you are not legally bound to provide your SSN to private sector entities. So, if a business requests your SSN, ask if it has an alternative number that can be used instead. Speak to a manager or supervisor if your request is not honored. Ask to see the company's written policy on SSNs. If the company does not have a policy or you are uncomfortable disclosing your SSN, take your business elsewhere.

Your Social Security Number

- Do not disclose your Social Security number (SSN) except when absolutely necessary to receive certain service or as required by law or (e.g. on tax forms, employment records, most banking, stock and property transactions).

- Whenever any business or organization asks you for your SSN, ask them why they need it, and request that an alternative method of identification be used.

- If your state I.D. contains your SSN as a method for identification, ask to use a substitute number.

At Work

- Do not provide your home address or telephone number for inclusion on a phone directory. Only give this information to those who absolutely need to know it.

- If possible, have any correspondence from work sent to your P.O. Box as opposed to your home. In the alternative, have all correspondence delivered to your work address.

- Inform yourself about information security procedures and policies at your workplace.

Employer's tools, employer's rules

Generally, employers retain access to and control over employer supplied or owned equipment. The law regulating employer access to and monitoring of communications and computer use is evolving. But, generally, employers may monitor and record employee communications, including email, if the monitoring occurs in the ordinary course of business or with the employee's actual or implied consent. Thus, your personal information communicated through any electronic means or stored on your work computer, as well as your Internet surfing and other computer activities may be accessed, monitored and recorded by your employer. This information may also be vulnerable to unauthorized access and disclosure by other employees.

The Family Educational Rights and Privacy Act (FERPA): Parents Are Not Powerless

FERPA is a federal law that protects the privacy of student educational records and gives parents and eligible students (in most instances that means adult students) certain rights including the right to inspect, review and correct erroneous information contained in the student's education records maintained by the school and the right to limit the disclosure of the student's information to others.

FERPA allows a school to disclose, without consent, "directory information," that may include the student's name, address, telephone number, date and place of birth, email address, and other information. However, the school is required to provide parents and eligible students notice detailing the directory information and disclosure policies and provide a means to opt-out of directory information disclosures. The methods for opting out are determined by the administration of each school. So, it is up to you to pro-actively look for and take advantage of the school's opt-out opportunities.

Special Concerns For Kids

You should teach your child:

- His or her full name, address and telephone number but remind them to only give it out to teachers or police-man and not to strangers or anyone they meet online.
- Not to tell strangers what you do for a living.

For schools, sports teams and other organizations:

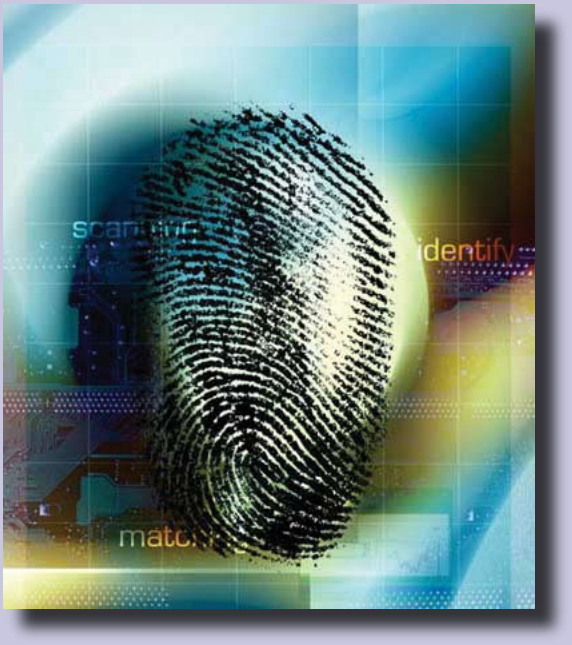
- Have your child use your office or cell phone as a contact number.
- Do not list your home address or telephone number in any school directory that may be distributed to others.
- Make teachers and coaches aware of the added security precautions necessary because of your position and ask them to be vigilant as well.

Protecting Childrens' Online Privacy

- Educate your children about the dangers of providing any personally identifiable information about themselves or family members to anyone – especially to anyone online.
- Instruct your children to never give out your last or family name, your home address or your phone number in chat rooms, on bulletin boards, or to online pen-pals.
- Instruct your children to never tell others their screen name, user ID or password.
- Be aware that by law, websites must get a parent's permission before the site can collect personally identifiable information from children who are under 13 years of age.
- Become familiar with the rules regarding children's online privacy protections. See **www.ftc.gov/privacy/privacyinitiatives/childrens.html** for more information.
- Look at a website's Privacy Policy to see how the site uses the information it collects.
- Avoid putting computer equipment in a child's bedroom. Whenever possible, set up computers, especially those with internet access, in a family room or other non-private area of the home.
- Know what sites your children are visiting. Whenever possible, children should surf the Internet with their parents.
- Ask to see any information your child has volunteered to any website.

Special Concerns For Judges

Federal Judges Financial Disclosures



The Ethics In Government Act of 1978 requires that, among others, all Federal judges make yearly disclosures of their finances to avoid potential conflicts of interest. These disclosures include information about non-investment income, gifts, liabilities, investments and trusts, reimbursements for value related to travel, and positions held outside of the federal government.

Your financial disclosures are retained by the Federal government for a period of six years. Thirty days after filing, they are made available to the public. Unlike executive and legislative financial disclosures, judicial financial disclosures are subject to a redaction policy. When a member of the public requests a specific judge's financial disclosure, the judge is notified of the request, and is allowed to request that certain types of information be redacted prior to sending the disclosure to the requester.

Redaction requests are generally approved if they pertain to information that may compromise the judge's physical or financial safety. Information that may compromise physical safety include unsecured locations of rental property or other real estate where the judge or the judge's family may be located, unsecured locations where children attend school, and the places of employment of spouses and children. Information relating to financial safety can include information that may make a judge more open to identity theft, such as account numbers, and information that may make a judge vulnerable to extortion or blackmail, such as the value of specific assets.

While financial disclosure reports are officially retained for six years, they may be publicly available for much longer. Certain court reform or watchdog groups like Judicial Watch and Courting Influence obtain these reports and maintain online archives of these documents. Not only does this mean that citizens can obtain them without following the standard request procedure, but it means that they are generally kept online well beyond the six-year retention period, perhaps indefinitely. If most of the sensitive information in your disclosures is redacted, then there is little risk, however, many of these watchdog groups will request each year's disclosure. If you feel that information in your disclosures could be used to locate you or your family, requesting its redaction may be wise.

Illinois State Judicial Candidate and Judicial Disclosures

In the State of Illinois, judicial candidates must make two different information disclosures: the petition packet and the statement of financial interest. The petition packet, which includes the judge's name, party and home address is submitted to the State Board of Elections. This information is officially retained for six months, but is left on the State Board of Elections website indefinitely. This includes the home address of all sitting judges and all losing candidates.

Sitting judges who wish to run for retention must resubmit their information to the State Board of Elections, which is then posted online.

In addition, an Illinois judge's Statement of Economic Interest must be filed with the Illinois Secretary of State. This information includes business interests in companies doing business in Illinois, professional organization employment, professional services rendered, capital assets with expected gains, relationships with lobbyists, gifts, and other governmental employment. This information is available to the general public upon request. In addition, statements from the last two years are available on the Secretary of State's website, and older disclosures are archived onto microfilm. The Index Division of the Secretary of State's Office is responsible for archiving the disclosures, and releases them to the public upon request. There is no limitation on releasing the information based on the age of the document, and the Index Division does not destroy files in its archives.

Resources

Optoutprescreen
(Processes consumer requests to prevent Consumer Credit Reporting Companies from providing credit file information for firm offers of credit or insurance that are not initiated by the consumer.) **www.optoutprescreen.com**

Annualcreditreport
(The official site to request a free annual credit report.) **www.annualcreditreport.com**

Federal Trade Commission
(Provides a wealth of online consumer protection and privacy-related information.) **www.ftc.gov**

Federal Communications Commission Consumer and Governmental Affairs Bureau
(Provides online information concerning communications privacy.) **www.fcc.gov/cgb/**

Electronic Privacy Information Center
(Public interest research center concerned with civil liberties in the information age.) **www.epic.org**

Electronic Frontier Foundation
(A nonprofit group working to protect digital rights.) **www.eff.org**

Privacy Rights Clearinghouse
(Nonprofit consumer information and advocacy organization.) **www.privacyrights.org**

The John Marshall Law School Center for Information Technology and Privacy Law
www.citpl.org or **www.jmls.edu**

Glossary

Anti-Virus Protection – a computer program designed to detect and respond to computer viruses and other malicious software. When implemented, anti-virus programs search files for intrusive viruses and irregular activity that may suggest the presence of viruses. Once a virus is recognized the program either repairs the infected file, isolates the affected file so the virus creates no further damage, or deletes the file altogether.

Blog – a contraction of "weblog" or "web log." It refers to a type of website consisting of frequently updated, chronological publications of comments and thoughts often in the form of journals or diaries.

Bluetooth – a technical industry standard for cable-free connectivity between wireless devices such as mobile phones, personal digital assistants (PDAs), handheld computers, wireless enabled laptop or desktop computers and peripherals. It uses short-range radio signals to link devices without wires over short distances. One common example of a Bluetooth device is the wireless headset for cellular phones.

Cookie – a small piece of data that certain websites attach to a user's hard drive while the user is browsing the website. A Cookie can contain information such as user ID and other personal information, user preferences, Web pages visited, and prior purchases. This data identifies users when they return to the website and allows for a more interactive browsing experience.

Data Broker – a company that collects and resells information about individuals. Data brokers package personal information in a variety of ways creating targeted customer lists, profiles and may other products for sale to marketers, government entities and others. Data brokers collect most of their information from public records, but may also cull information from other sources such as consumer credit reports. Current privacy laws provide very few limitations on the activities of commercial data brokers. Also known as information broker or data aggregator.

Domain Name – a unique "address" or Uniform Resource Locators (URL) that identifies a particular website. Domain names have two or more parts separated by dots. **www.chicagobar.org** for example. A domain name can be found to the right of the @ sign in an email address.

Encryption – the process of scrambling data by means of a mathematical formula or algorithm that prevents an unauthorized party from reading or changing the data.

Firewall – hardware or software that protects the resources of a private computer network from users from other networks. A firewall can prevent unauthorized access or potentially dangerous material from entering the system. The term may also refer to the security policy that is used with the software or hardware.

Internet – the worldwide, publicly accessible network of interconnected computer networks consisting of millions of smaller academic, business, and government networks. This network of networks carries a range of information and services including email, file sharing, file transfer and linked Web pages and other documents of the World Wide Web.

Land Trust – a legal instrument that allows a property owner to effectively remove his or her name from the public record by transferring title of the real property to a trustee to hold for the benefit of a beneficiary i.e., the actual owner. Because the beneficiary of the land trust is not recorded as such in the public record, establishing such a trust effectively obscures one's relationship to his/her real property.

Loyalty Card – a plastic card, or other object, that identifies the holder as a member as a frequent user or part of a commercial incentives or discount program. Often, the consumer must provide the issuer personal information in order to participate. Also known as a frequent shopper card, rewards card, points card, or club card.

Opt-in – a permission-based method used in marketing and information sharing that requires data subjects to explicitly consent to receiving advertisements or having their information shared with others.

Opt-out – a method used in marketing and information sharing requiring data subjects to explicitly deny permission to receive advertisements, services or have their information shared with others.

Personal Digital Assistant (PDA) – a handheld device, originally designed as an electronic personal organizer (to replace paper calendars and date books), that may now contain many features in addition to calendars such as clocks, calculators, phones, Internet browsers, and email clients.

Personally Identifiable Information (PII) – information that can be used to identify, contact, or locate a specific person. Examples of PII include your full name (especially if it is not a common name), telephone number, street address, driver's license number, credit card numbers, Passport numbers, bank account information, employee identification cards, biometric information (fingerprints, DNA, etc) and social security number.

Phishing – a fraudulent activity that attempts to induce victims to volunteer sensitive information, such as passwords, account numbers or credit card details, by masquerading as a genuine communication from a legitimate business. Phishing is most often accomplished through email. Phishing may also involve "pharming," which redirects a legitimate website's traffic to another, illegitimate or fraudulent website.

Pretexting – the practice of obtaining personal information under false pretenses. Pretexters often pose as someone authorized to access an account and attempt to bluff their way into obtaining information such as passwords, or account numbers from financial institutiuons, phone companies or other data holders. Pretexting to obtain financial information is illegal.

Public domain – the body of knowledge and innovation to which no person or other legal entity can establish or maintain proprietary interests. This body of information and creativity is considered to be part of the common cultural and intellectual heritage of humanity, which in general anyone may use or exploit.

Public record information - information that is collected and maintained by various government entities that by definition, operation of law or long-standing tradition, are open to the public for inspection. Examples of public records include real estate transactions, business ownership, court filings, and marriage and death certificates.

Publicly available information – information that is accessible to the general public from a number of non-governmental sources including newspaper articles, telephone directories and websites.

Remote access programs – software that allows users to access their home or office computers from remote locations. Programs like PCAnywhere, Laplink, and Timbuktu are "remote access" programs. These programs may pose security risks and may be vulnerable to attacks by malicious computer hackers.

Shoulder surfer – a slang term for people who attempt to steal passwords and PINs from others by secretly observing others entering the information. Shoulder surfers may accomplish this by obvious means such as standing behind their target, or they may employ devices that allow them to view multiple people from a safe distance.

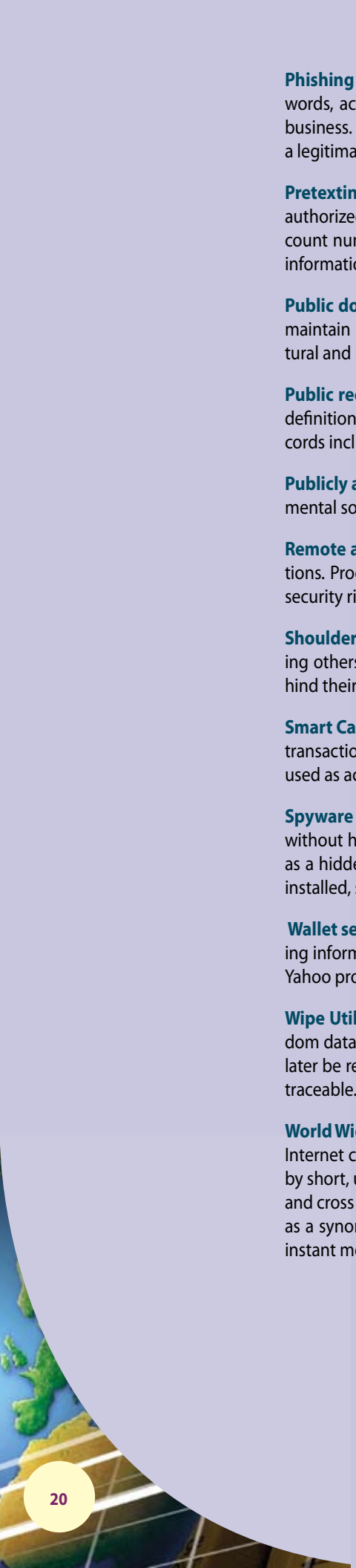
Smart Card – a plastic or other device with a built-in microprocessor and memory used for identification or financial transactions. Smart cards typically hold account information, passwords or other personal information. They can be used as access cards, cash cards or credit cards with a preset credit limit.

Spyware – software that covertly gathers user information and activities through the user's Internet connection without his or her knowledge or consent, usually for advertising purposes. Spyware applications are often bundled as a hidden component of free downloadable software, but can also be acquired through computer viruses. Once installed, spyware collects information and transmits that information back to a third party.

Wallet services – services or software that store your user names, passwords, credit card information, and other billing information to make online shopping faster and more streamlined. Companies such as Microsoft , Motorola and Yahoo provide services of this type.

Wipe Utility – software that completely destroys data by overwriting and replacing the hard disk surface with random data. Because files are not entirely removed from a computer when they are conventionally deleted, they may later be retrieved. A Wipe Utility Program effectively renders files and data contained in them irrecoverable and untraceable.

World Wide Web (Web or WWW) – a global system for browsing Internet sites. The world wide web is a portion of the Internet comprised of a collection or "web" of many sites linked together by a common protocol. Sites are identified by short, unique identifiers called Uniform Resource Locators (URLs) that allow each site to be easily found, accessed and cross referenced. Not all Internet servers are part of the World Wide Web. The term "web" is often mistakenly used as a synonym for the Internet itself, but the Web is actually something that is available via the Internet, like email, instant messaging, file sharing, many other Internet services.



Top 15 Tips To Protect Your Personal Privacy

1. Keep your information private and only share your personal information when absolutely necessary.
2. Disclose your home address only to trusted third parties or when required by law. If you must give out an address, use your office address or a post office box whenever possible.
3. Opt-out, opt-out, opt-out. Take advantage of opportunities to restrict the sharing of your personal information with others.
4. Do not participate in surveys, warranty cards, store discount cards, online contests or giveaways.
5. Have a "non-published" or "non-listed" residential telephone number
6. Deposit outgoing mail in post office collection boxes or at the post office. Install a locked mailbox at your residence to deter theft of incoming mail.
7. Shred all documents you throw away that may contain your personal information. A cross-cut shredder is preferable.
8. Read website privacy policies
9. Unless you have initiated contact, do not divulge personal information over the phone or the Internet.
10. If permitted by state law, put real estate you own in land trusts.
11. Use firewall, anti-spyware, anti-virus software, and spam filters on PCs.
12. Use secured wireless and Internet network connections.
13. Never leave your computer unattended after logging in with your password.
14. Do not disclose your social security number except as necessary and required by law.
15. Educate your children about the dangers of providing any personally identifiable information about themselves or family members to anyone – especially to anyone online.

Publication Credits

Protecting Your Personal Privacy: A Self-Help Guide for Judges and Their Families **was published by The Chicago Bar Association's Privacy Task Force and the John Marshall Law School Center for Information Technology and Privacy Law. © October 2006. Editor and Principal Author: Leslie Ann Reis. Contributing Authors: Priya Krishnamoorthy Venkat, Matthew Hector, Richard C. Balough and David E. Sorkin. Researchers: Christopher Bojar and Ryan Kaiser. Design: David M. Beam.**