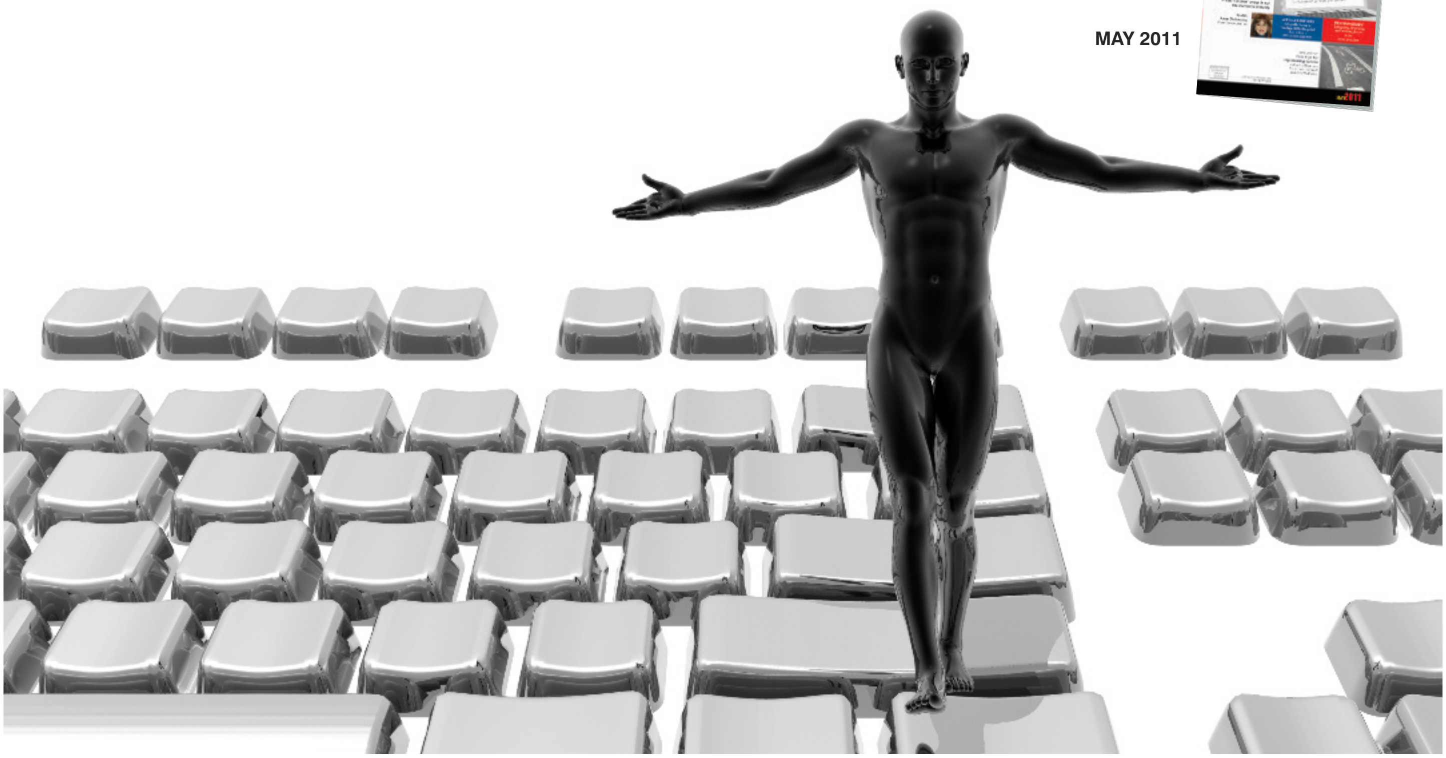


Surf the Net invisibly, instead of naked

Protect yourself and your clients from snoops and Internet bandits. Advice on how to protect your identity when searching the net, and how to cleanup your PC afterwards

Mortimer

By Michael Mortimer

In this article I will discuss how effectively to surf the Net invisibly, the reasons you might want to do so and its benefits, including protecting yourself from online criminals and snoops.

In addition, I will explore the problems – the risks and exposure you face whenever going on the Net – and then review the software and service I recommend: *Windows CleanUp* and *Hide My IP,* which I have purchased and been testing for nine months.

What is an IP?

"IP" is short for "Internet protocol." Obviously, in a lawyers' magazine I can't talk in technical terms about what that means (besides, who wants to read that technical stuff); what I tell people is to simply think of an IP as a sort of telephone number. An IP, just like your phone number, is a unique identifier assigned to your modem and account by your Internet Service Provider ("ISP").

Wondering what the IP is of the computer Net connection you are currently using? It's easy to find out. Simply log on to one of these sites, and they will display it: ipf1.com or formyip.com (or you can use Google to search the term: "What is my IP").

Note: An IP is *not* assigned to a computer. An IP number comes from your Internet Service Provider (in the San Francisco Bay Area, most likely AT&T or Comcast) and tied to the modem the ISP gave you when you signed up for Internet service.

An IP will only work with the account assigned to the IP. In other words, if your ISP at the office is AT&T and Comcast broadband at home, you will have an IP for the office modem and a different IP for the home broadband connection.

Invasion of the privacy snatchers: Net criminals

Unless you "clean up your IP act" and scrub your computer's temporary memory, sophisticated low-life dirt bags with malicious intent are going to get information about where you are located, who you are, your computer configuration and even what programs are running on your computer.

If you don't take protective measures, businesses and IP criminals are exchanging dossiers containing a list of your daily activities, including your bank transactions, shopping habits, passwords entered, whom you owe money to, your financial status, what time you go to bed, what time you get up, when you leave your house and where you work.

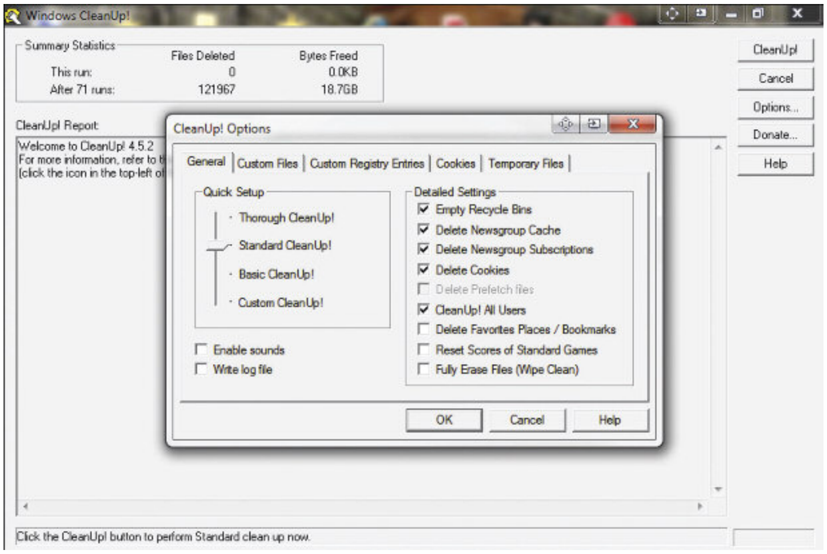
•Profilers – If you use the Internet, there are Web sites and individuals who, for business purposes, semi-nefariously (my opinion) detect your IP and then track your Internet use.

They do this to build an Internet dossier or profile on you.

It's pretty easy to do, too. Companies use software and humans to "grab" your IP and from there to detect or track everywhere on the Net your IP has been and everything that your IP has done, including downloading data such as music or movies. End result, individuals and businesses can get a very detailed profile on who you are and what you do.

Vignette: In year 2001 I had a client who wanted to know about taxes on his upcoming settlement. In 2002 I had a client who wanted to know about filing bankruptcy on his business. In both these situations, I went online and searched for information. (At the time I was not using memory cleaning software to the extent I do now, which is every day. The "fake IP" services were turtle slow back then, so I did not use them.)

Because of the above Net travels, ten years later I am still receiving SPAM e-mail related to the issues I had researched on behalf of those clients. Clearly what had happened is that someone, after digging around in my computer's temp memory, had harvested the private information residing in my computer's cache that I carelessly had left resident in the temp memory for all to see.



Summary Statistics

	Files Deleted	Bytes Freed
This run:	0	0.0KB
After 71 runs:	121967	18.7GB

CleanUp! Report

Welcome to CleanUp! 4.5.2
For more information, refer to t
(click the icon in the top-left of

Quick Setup

- Thorough CleanUp!
- Standard CleanUp!
- Basic CleanUp!
- Custom CleanUp!

□ Enable sounds
□ Write log file

Detailed Settings

☑ Empty Recycle Bins
☑ Delete Newsgroup Cache
☑ Delete Newsgroup Subscriptions
☑ Delete Cookies
□ Delete Prefetch files
☑ CleanUp! All Users
□ Delete Favorites Places / Bookmarks
□ Reset Scores of Standard Games
□ Fully Erase Files (Wipe Clean)

Click the CleanUp! button to perform Standard clean up now.

Figure 1: The Windows CleanUp options menu allows you to get quite aggressive in how deep the program should clean the computer. Until you learn about the features, use the program's default settings.

The information harvested, by the way, includes bookmarks, Web site addresses, image files, and even thumbnails of documents exchanged in e-mails.

•Net banditos – In addition to businesses who want your information to market products, another more sinister group is hunting the Net for your confidential data, those individuals called cyber or Net criminals. These are creeps with malicious intent, focused on finding ways to rip you off. They know how to use programs to search the Internet for "open ports" that enable them to eventually seize control of your computer (usually via an installed Trojan).

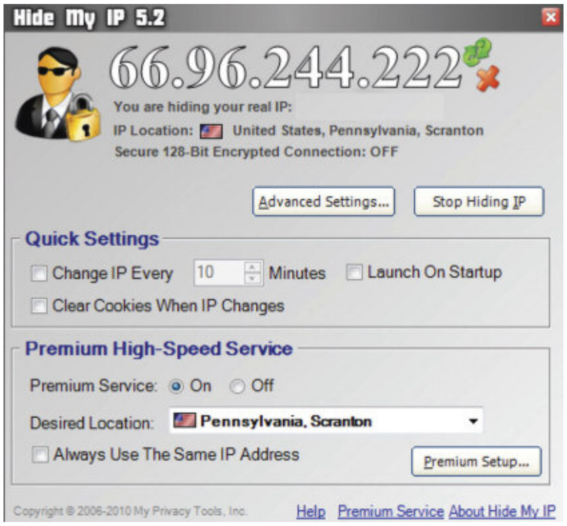
And sadly it's getting worse because, as covered on the news or *60 Minutes*, criminals have modernized and moved to the Internet, mainly because it's a low overhead operation and the Net provides far more fertile ground within which to ply their trade. What should keep you awake at night is the knowledge that cyber criminals are experts at picking your computer pockets (that is, "pockets" in the form of "temporary memory banks" and "silicon repositories").

Bonus Warning: You should additionally be concerned because clients use the Internet. Nowadays e-discovery requests include a demand to see your client's computers so that the opposition can find incriminating or impeachment evidence.

It does not take much of an imagination to envision a trade-secret thefts' prosecution going quite well (due to your brilliant maneuvers), only to have the case morph into a zero-value dog because of Internet evidence defense counsel found on your client's computer.

Solutions and tools

In addition to antivirus and firewall software that I use on my computers as defensive measures, there are two programs I use to act invisible when I am conducting research on behalf of a client, sleuthing around the Net, browsing on



Hide My IP 5.2

66.96.244.222

You are hiding your real IP:

IP Location: United States, Pennsylvania, Scranton

Secure 128-Bit Encrypted Connection: OFF

Quick Settings

□ Change IP Every 10 Minutes □ Launch On Startup

□ Clear Cookies When IP Changes

Premium High-Speed Service

Premium Service: ● On ○ Off

Desired Location: Pennsylvania, Scranton

□ Always Use The Same IP Address

Copyright © 2006-2010 My Privacy Tools, Inc.

Figure 2: The HideMyIP graphical interface is intuitive and easy to use. Double click the program icon which can be set to automatically hide your IP.

the Net, or assuring that Net scammers won't get private information because it's residing in my computer's temporary memory.

Program #1 is freeware, albeit the developer requests donations. It's called *CleanUp*! You can download it here: tinyurl.com/PMCleanUp.

CleanUp does what the name implies, it quickly cleans your computer of any information residing in your browser's or e-mail's temp memory. It cleans out Web addresses you have visited, e-mail addresses you have entered, passwords, account numbers, user names, etc.

Program #2 is a service that requires installation of a small application interface on your computer. It's called *Hide My IP* and depending on features/options ordered, the service can cost you from $30, $110, to over $300 annually. The product/service Web site is here: hide-my-ip.com.

Hide My IP too does exactly what the name implies; it hides your Internet Protocol number. Think of *Hide My IP* as turning you into the invisible man or woman. It's like making your IP number "unlisted" in the phone directory or activating your cell phone's caller ID block feature.

Full Disclosure: To remain unbiased, like Consumer Reports, I do not accept anything for free from companies whose products or services I review. I pay for everything out of my own pocket. So my product reviews and recommendations get their start by opening my wallet just the same as you do.

Additional benefits of using an IP masking service

Besides the cool factor one enjoys when surfing anonymously, there's other benefits to using *Hide My IP*.

For example:

- Conducting investigations into enemy territory. E.g., on a case, I was looking for impeachment evidence on a defendant witness. This required my snooping around defendant's Web site. The concern I had was that Defendant's counsel was sharp as a tack, so I knew the defendant's IT people might check to see if I visited the Web site and obtained documents useful for impeachment of a defendant vice president whom I subpoenaed to testify at trial. End result: I did in fact find a PowerPoint presentation on defendant's Web site that contradicted the defendant's discovery responses and that was at the ready for use at trial to impeach the defendant witness. Defendant was none the wiser that I had snooped around its Web site and had an impeaching document.
- Some forums and blogs are restricted sites, where they ask for an e-mail, phone number and other identifying information. A throwaway g-mail account and masked IP are valuable in letting you infiltrate Web site forums, while keeping your personal information private.
- Many file download sites restrict free downloads to one file per hour, for example. A site enforces the limit by reading your IP. If your IP is exceeding the site's limit, it blocks your IP and download. Solution: Close your browser, use *CleanUp* to clear your cookies and cache, use *Hide My IP* to get a different IP and go back to the site to download the files you need.
- Did you join a forum or blog that discusses politics or religion? Did you anger the forum owner to where he banned your IP? No problem, use *Hide My IP*, get a different user name and you can rejoin the site to anger them again. Note: if you use this workaround, make sure your subterfuge is complete. Come up with a different user name, password and e-mail address. If you use any of these that are similar to your banned information, the site owner will bust your butt and send out henchmen to fix your wagon for good.
- The saying goes, "At the Thanksgiving table never bring up politics or religion" (unless you don't mind fisticuffs for dessert). The same goes for your law practice. Never discuss politics or religion with a client. Because some prospective clients Google the lawyer to find out her views or other information, never use your real name as a user name when joining forums or blogs. In other words, don't leave Net tracks that might offend a prospective client. (And don't leave your fingerprints on the Net, so to speak, that tells people in the profession you are nuttier than squirrel droppings.)
- Using an IP mask, cache cleaner and not entering ID information are excellent ways to reduce the amount of SPAM to your e-mail accounts. By "keeping things clean," there's nothing for the spammers to harvest, capture, or steal.

Bonus tips

- *Hide My IP*, like many programs, is designed to get you hooked or addicted to the service, then they hit you with come-ons for additional features. (Can you spell "Apple" and "Steve Jobs?") The base price for the service gives you acceptable service, but for an additional $80 annually you can get a Premium Account. The

Premium Account is excellent. It works quite fast to establish a fake IP connection, and the service is reliable.

- *Hide My IP* detects the computer on which you have installed the service software (that is, the program installed on your computer to call up *Hide My IP*'s servers). Your payment allows use on only one machine. If you want to install *Hide My IP* on multiple machines, you need to buy additional licenses.
- Once you start your anonymous online session do *not* open any Web site to input your e-mail address, telephone numbers or other identifying information. If using forums or blogs that require registration, get a "throwaway" G-Mail free e-mail address.
- Remember, just because you are hiding your IP, this does *not* mean that someone cannot access your keystrokes or any information you input. Although they probably can't, assume people can access your computer, by installing a Trojan or whatever and keep an eye on things.
- Many of your important accounts (banks, credit cards) recorded your IP when you registered with the institution to gain online access. Because of this, when you access super secure sites, servers match up your user name, password, and check your IP. If the IP is suspicious looking or unfamiliar (e.g., your IP indicates you are in Madagascar, a place you are not in and never will be) the institution may ask you a security question to gain access. For example, when I forget to log off *Hide My IP*, when I try to log on to my bank a message pops up saying, "We are concerned about your security. Please tell us the name of your grandparents." After I answer "Grandpa Neander and Grandma Thal," I can log into my bank account.
- IP hiding software is *NOT* anti-virus or firewall protection. If you visit malicious Web sites (defined as a Web site where someone will attempt to crack into your computer) do so at your peril. Malicious hackers and crackers may still be able to get to your computer, especially if you don't have updated antivirus and firewall protection.
- After your anonymous session is over, *you need to run your cleaning program.* This is because there may be temporary files that have been planted on your computer, such as cookies, images, Web pages and other "paper trails" showing where you have been, what you have seen and what you have done.
- Usually rebooting your computer will *not* wipe your tracks. You must use a program like that I recommended in here (*Windows CleanUp*).
- Criminals love people who leave their computers on for days at a time, never reboot and don't clean up their tracks. Those computers are a treasure trove of information such as passwords, physical addresses, account numbers, phone numbers, e-mail addresses and other private information. Don't do as I recommend in here, so that the nefarious will get a bead on *your* computer rather than mine.
- While "in session" using *Hide My IP* and *CleanUp,* don't enter sensitive information on Web sites and especially don't check your e-mails.
- Some sites, not necessarily banks or financial institutions, can detect that you are using a "proxy server," "fake IP," or "IP mask." When trying to access those sites, e.g., to post a comment on a blog, a message may pop up saying words to the effect: "Sorry, this site forbids use of proxy servers or other ID masking programs." There's ways around that but the space limitations of this article prevents me from going into that much detail.
- All the IP masking services charge by the year, typically. I am unaware of any stand-alone software or program that provides masking services at the cost of the software. That would not work anyway because masking services rely on computers, servers and live people to keep everything updated.

Pricing models are all the same too. The more money you pay, the faster the Net surfing experience, and the more locations (servers) that are made available to you.

- BEWARE: Some companies providing IP masking are fly-by-night con men who try to take in as much money as possible, and then eventually they close down the business. To placate people who first sign up, they provide minimal service, meaning the IP masking servers are molasses slow.
- Over the years the main complaint I have had about other "fake IP" companies is that the servers have been so slow. In contrast, *Hide My IP* is so fast that many times I have forgotten to log off after I am done with an anonymous session.
- Although *Windows CleanUp* is free of charge and the program is ad-free, the developer has a donate button on the program's interface. I donated $25. Let your conscience be your guide when making a decision on donating, or not.

Conclusion

Reading this article evidences that you are extremely competent and possess common sense. So you no doubt know that there are hundreds of people and businesses who know exactly where and who you are (utility companies, auto insurer, wireless and landline phone services, cable TV company, and yes, even your ISP providing you with an IP).

You may be wondering what the point of *Hide My IP* is if everyone knows who you are.

Well… an IP masking service is NOT to allow you to hide from the State Bar, law enforcement, nor to lay low from society and business. Programs like *Hide My IP* and *CleanUp* are used to protect you from strangers lurking on the Internet, the wrongdoers who harvest your personal information and sell it to others.

These programs and services can also thwart criminals looking for users "surfing in the nude," people who don't reboot their computers, never clean the temp file folder or don't use up-to-date antivirus or who don't know what a firewall is for.

Remember, make it difficult for Internet snoops and criminals to see you. And don't leave any information in the "vault" for them to steal; that is, if they gain access to your computer's memory. If they can't see you or there's no information to

harvest, these nefarious types will ignore you and move on to easier targets, of which there are plenty.

Besides, I have to admit when I am surfing invisibly, sleuthing around, or knowing that I am defeating the wicked and criminal at their own game, I get a feeling of empowerment and actually believe what others for years have said about me: I am truly master of all I survey.

Michael Mortimer is a federal trial lawyer located in San Francisco. He is spending most of his time now authoring a number of books including Welcome to the World of Big Time Litigation. *Mortimer is also the regular technology columnist for* Plaintiff Magazine. *You can e-mail him at sanfrancisco@att.net.*