Free Privacy Guide

The 5 easiest ways to
get more privacy.

Bill Rounds, Esq.
Trace Mayer, J.D.

THE FREE INTRODUCTORY GUIDE TO PRIVACY:

Why You Need Privacy And Free Things You Can Do To Protect It

ABOUT THE AUTHORS

Trace Mayer, J.D., author of The Great Credit Contraction holds a degree in Accounting, a law degree from California Western School of Law and studies the Austrian school of economics.

He works as an entrepreneur, investor, journalist and monetary scientist. He is a strong advocate of the freedom of speech, a member of the Society of Professional Journalists and the San Diego County Bar Association. He has appeared on ABC, NBC, BNN, radio shows and presented at many investment conferences throughout the world.

Bill Rounds, J.D., is a California attorney and holds a degree in Accounting from the University of Utah and a law degree from California Western School of Law.

He practices civil litigation, domestic and foreign business entity formation and transactions, criminal defense and privacy law. He is a strong advocate of personal and financial freedom and civil liberties.

> Protections for anonymous speech are vital to democratic discourse. Allowing dissenters to shield their identities frees them to express critical, minority views . . . Anonymity is a shield from the tyranny of the majority. . . . It thus exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation . . . at the hand of an intolerant society.
>
> Justice John Paul Stevens, McIntyre v. Ohio Elections Comm'n[1]

WELCOME NEW READER!

Now that you have discovered HowToVanish.com you can become a part of a growing community of people concerned about personal and financial privacy. There are many legal and ethical reasons why someone would be concerned about their privacy. I want to give you a tool that you can use to rate yourself on how well you are protecting your own privacy and then show you five basic but powerful things to do to increase your own privacy protection right away.

[1] McIntyre v. Ohio Elections Commissions, 514 U.S. 334 (1995).

PERSONAL SAFETY

People may desire privacy for personal safety. People whose professional life is very public, such as politicians, school teachers, police officers, celebrities or industry leaders, are regularly subjected to public criticism. Criticism can sometimes mutate into something more sinister. Cape Fear's fictional villain stalked and harassed the family of his prosecutor from years earlier.[2] In real life, celebrities and their families face dangerous encounters with deranged fans, like the stalker who showed up at the home of Gwenneth Paltrow's parents. In the US and in Kyrgystan, family members of unpopular and immoral politicians have been the target of harassment, violence and intimidation. The risk to all of those people, their family and their friends, could have been mitigated with adequate privacy practices. In most cases, even the most simple methods of privacy protection would have deterred all but the most well funded and rabid stalker.

FINANCIAL SECURITY

There are a host of financial incentives to maintain privacy, especially where there are corrupt governments, risk of kidnapping for ransom, extortion, and abusive litigation. Every year, millions of people are victims of identity theft. Their personal, medical, financial

[2] United States of America v. Talley, 2008 U.S. App. LEXIS 21764.

and other information is stolen, used for nefarious purposes and they suffer serious consequences. Identity theft doesn't only happen because people are careless with their own information. Many times third parties collect valuable personal information and do not properly safeguard that information. Criminals can steal your credit card number from your credit card company if they can't steal it from you.[3] You can reduce the probability of being a victim of this maddening crime by sharing less personal information with third parties and decreasing access points to personal information.

CORPORATE DUE DILIGENCE

Corporate espionage is big business. Ideas flowing within and among corporations can be worth billions and needs to be protected.[4] Even small businesses with strong competition can live or die by the information divulged between competitors. Businesses cannot rely on the law to protect their valuable information, ideas and data. People break the law all the time. Like locking your door to prevent burglary, something

[3] United States v. Gonzalez, No. 09-CR-10262 (D. Mass).

[4] United States v. Min, No. 06-CR-121 (D.Del).

that is already illegal, business people need to rely on technologies and techniques to protect their valuable ideas and information. In many cases, the officers and directors owe a fiduciary duty to use proper privacy protection.

BIG BROTHER IS WATCHING

Despite centuries of experience many people are under the delusion that government officials always work in the best interest of citizens. They forget that the leading cause of non-natural death in the 20th century were governments.[5] Whether governments waged war on individual's privacy by forcing them to wear stars of David on their arms or carry government issued cards identifying them as Tutsis the involuntary disclosures were tools used to perpetuate state sponsored genocides. In far too many cases the 'protectors' have become the exterminators. For example, the self-hallowed United States used census data to round up hundreds of thousands of innocent American citizens and force them into concentration camps[6] while vaporizing hundreds of thousands of their relatives.[7] Even the United Nations has proclaimed,

> No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."[8]

Noble and honorable men like Sir Thomas More have even paid with their life in defending the ideal of equity, justice and law.

---

[5] USA, France, UK, and USSR v. Hermann Goering et al., Nuremberg Trials 1945-46.

[6] http://en.wikipedia.org/wiki/Japanese_American_internment.

[7] http://en.wikipedia.org/wiki/Atomic_bombings_of_Hiroshima_and_Nagasaki.

[8] United Nations International Covenant On Civil And Political Rights. Part 3 Article 17. 7 July 1994.

William Roper: So, now you give the Devil the benefit of law!
Sir Thomas More: Yes! What would you do? Cut a great road through the law to get after the Devil?
William Roper: Yes, I'd cut down every law in England to do that!
Sir Thomas More: Oh? And when the last law was down, and the Devil turned 'round on you, where would you hide, Roper, the laws all being flat? This country is planted thick with laws, from coast to coast, Man's laws, not God's! And if you cut them down, and you're just the man to do it, do you really think you could stand upright in the winds that would blow then? Yes, I'd give the Devil benefit of law, for my own safety's sake![9]

Despite the fanciful ideal that governments should exist to protect the privacy of the individual and not the privacy of government; the stark facts suggest that many people live in or visit countries where a nefarious Big Brother is watching. But neither China nor the United States are free and open societies. Their governments monitor Internet traffic and block or restrict access to a significant amount of vital information and interfere with the freedom of the press.[10] Both Massachusetts and Indiana have made it illegal to record any police officer in any circumstance and some states charge such whistleblowers recording police brutality with illegal wiretapping.[11]

Without knowing how to vanish, I doubt you can learn much. Fortunately, there are powerful tools of privacy available to avoid government surveillance of online activity, even in places like China. A good example of those tools in action was the recent citizen protests in Iran. Big Brother blocked Internet access to sites like Twitter and YouTube, but the information was spread throughout Iran and to the rest of the world using tools discussed in How To Vanish.

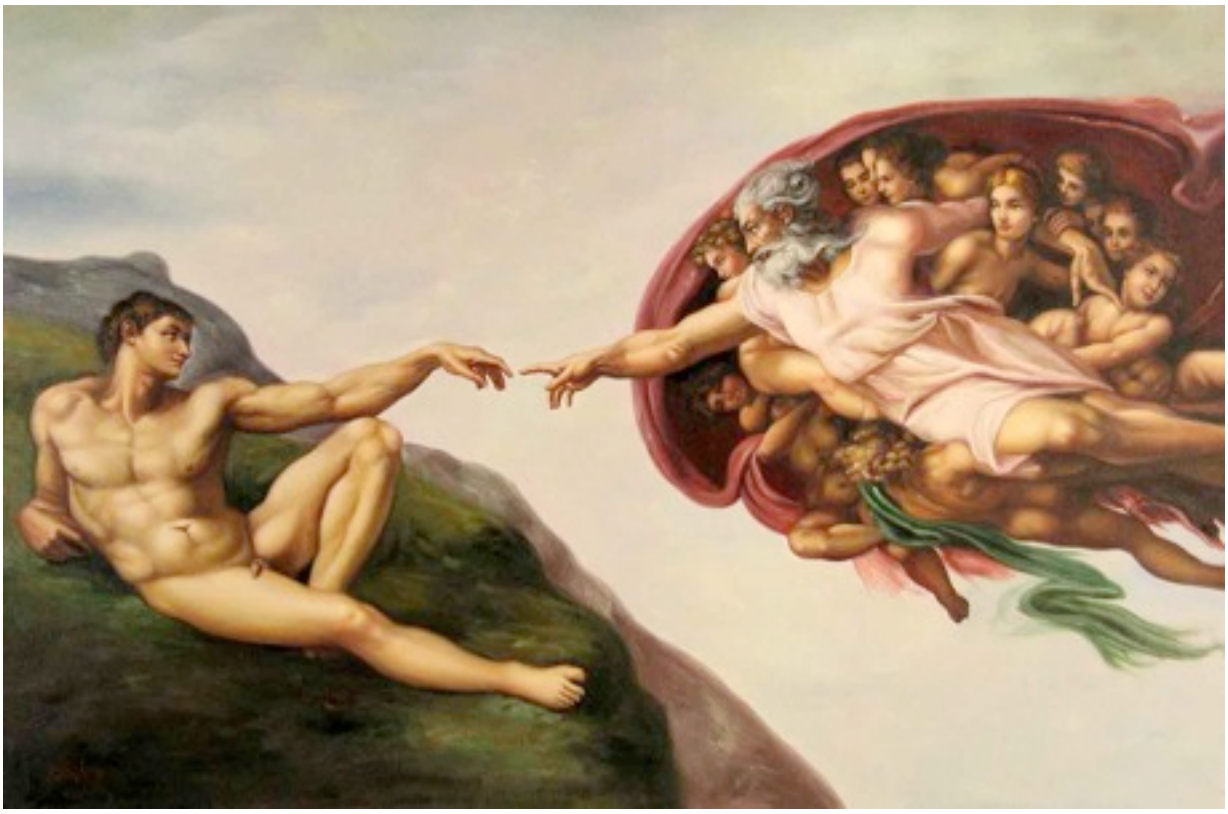
---

[9] A Man For All Seasons. Movie. 1966.

[10] http://collateralmurder.com/.

[11] Commonwealth v Hyde, 750 N.E.2d 963 (Mass. 2001).

A FUNDAMENTAL HUMAN RIGHT



The Declaration of Independence and the United Sstates Constitution does not give anybody any rights. Those documents only articulate some of the fundamental civil and human rights that we, as human beings, inherently have. They also establish the boundaries of what the government can legitimately do. Because individuals are endowed with human rights and because individuals create governments therefore it follows that governments may only morally and legitimately do at most what an individual can do. The creature cannot exceed the creator.

But governments always have, and always will, violate those rights to some extent. Privacy is fundamentally a civil and human right. But all rights, like your right to remain silent or your right to an attorney, can be waived if you are not careful.

How To Vanish is a tool to help you avoid unintentionally waiving your rights. Because the right to privacy is a civil and human right, some of the same tactics that have been used historically to fight violations of civil rights are useful in the fight for privacy. One of those tactics is a boycott.[12] HowToVanish.com shows you how to legally boycott the systems and institutions, both public and private, that violate your rights.

> Privacy is the right to be alone--the most comprehensive of rights, and the right most valued by civilized man.
>
> Louis D. Brandeis[13]

No matter what your reason, or combination of reasons, for wanting to protect your privacy, How To Vanish will help you move closer to your goal.

GETTING THE MOST BENEFIT

There are three components to making yourself more private. First, the **rules** and the **tools**. Knowing what things lead to a loss of privacy and what things lead to an increase in privacy is the first step to exercising your own civil right to privacy. The second step is **practice**. You must become familiar with how to use the rules and tools to your own advantage. For some rules and tools, application will be very simple and require very little effort. For others, you will need to practice their use a lot before you are competent enough to make them effective. Third, you have to have an overall **strategy** which will satisfy your goals of privacy. For this you need to know how to combine the effective use of the rules and tools so that they provide the kind of protection that you want at the price you are willing to pay.

---

[12] Browder v. Gayle, 142 F. Supp. 707 (1956).

[13] Olmstead v. United States, 277 US 438 (1928).

> Law-abiding citizens value privacy. Terrorists require invisibility. The two are not the same, and they should not be confused.
>
> Richard Perle

This free guide, HowToVanish.com, and the related products that are offered there, show you what the rules and tools are and how to use them. HowToVanish.com encourages you to practice using the tools and techniques so that you get good at wielding them. HowToVanish also gives you some examples of strategies that people have used or are using in order to achieve a particular privacy goal.

HOW PRIVATE ARE YOU NOW?

You might be surprised at how easy it is to obtain your personal information. You may or may not know how much of your personal information is available to anyone who is interested. You probably don't know where that information can be found. Take this quick survey to see just how you rate on a scale from D.B. Cooper to Lindsay Lohan to see just how public your private personal information might be. Give yourself one point every time you answer yes to one of these questions. If you answer no, you get no points. Add them up at the end and compare it to the scale.

ADDRESS

___ There is a name on your mailbox.
___ Your house number is visible from the street.
___ Anyone can approach your front door.
___ You receive mail in your own name at your residence.
___ You send mail from your street side mailbox.
___ You send mail from a blue USPS street side mailbox.
___ Your house is on a Hollywood map of the stars.
___ You use your home address for drivers license and other government documents.
___ You have posted your address somewhere public (eg: Craigslist, website, etc.)
___ You have packages sent to your home address in your name.
___ Your house is listed as your billing address on any accounts.
___ You have ever had pizza delivered to your house.
___ You own property in your own personal name (or a name easily identifying you).
___ You put your home address as the return address on outgoing mail.
___ You park your car in the driveway.
___ You don't have a 20 foot wall, a moat or attack dogs surrounding your house.

PHONE

___ You give out your home number regularly.
___ You make calls with a cell phone.
___ Your number is listed in any directory.
___ You Google your phone number and your name comes up (go ahead, try it).
___ You use a cordless phone.
___ Your phone service is in your own personal name.
___ You call people that record their calls.
___ You do not encrypt your calls.
___ Your area code is the same area code as your residence.
___ You have identifying information in your voicemail greeting.
___ You leave your cell phone on all the time.
___ You never take the battery out of your cell phone.

COMMUNICATIONS

___ You don't encrypt your email.
___ You don't have an enigma machine.
___ You don't use advanced code techniques for your written messages.
___ You use a password that is found in the dictionary.
___ Your password is less than 10 characters long.
___ You don't use numbers or symbols in your password.
___ Your password reminders are easy to guess.
___ You use password reminders that is public information (eg: where were you born).

OTHER ELECTRONICS

___ You use a color laser printer or an inkjet printer.
___ You click around in unsafe neighborhoods on the internet.
___ You have spyware or malware on your computer right now.
___ You don't know how to defragment a hard drive.
___ You donate or sell your old computer.
___ You don't have a firewall.
___ You don't have anti virus software.
___ Your anti virus software is outdated.
___ You use the internet.
___ You use Google.
___ You don't know what a proxy server is.
___ You open suspicious emails.
___ You download suspicious attachments.
___ You click on suspicious links in emails.
___ Your wireless router is not password protected.
___ You use public wifi hotspots.
___ You don't password protect your computer on startup.
___ You don't use a password protected screensaver.
___ You have never removed your hard drive and replaced it with a temporary one.

FINANCIAL

___ You have a US bank account.
___ You fit one of the many profiles of a criminal.
___ You pay for most things with check, or card.
___ You put personal info on a check.
___ You put an account number on a check when you pay a bill
___ You use your social security number for anything.
___ You receive marketing offers in your name.
___ You are a US citizen.

SOCIAL

___ You have a Facebook profile.
___ You have a Linkedin account.
___ You have a Myspace account.
___ You have a Twitter account.
___ You have posted a resume on a job hunting site like Monster.com.
___ You have any other social networking account.
___ You have more than one friend/connection on a social networking site.
___ Your profile on any social networking site has your actual pictures.
___ Your profile on any one of these has your actual birthday (either day or year).
___ Your profile on any one of these shows your actual city.
___ Your profile has low or default privacy settings.
___ You are tagged in photos that aren't flattering.
___ Your friends post unflattering pictures of you.

OTHER

___ You use your drivers license when asked to show identification.
___ You don't shred your trash.
___ You leave your trash by the curb.
___ You have never seen the video Busted: The Citizen's Guide To Surviving Police Encounters.
___ You have not seen the video Busted: The Citizen's Guide To Surviving Police Encounters more than 2 times.
___ You have not memorized the video Busted: The Citizen's Guide To Surviving Police Encounters.
___ You keep property in a safety deposit box.
___ You have ever hired a moving company.
___ Your car is registered in your own name.
___ You have medical insurance.
___ You are an employee of a company that you do not own.
___ You are in debt.
___ You are not living off the grid.
___ You disobey some traffic laws.
___ Your name is Lindsay Lohan (add 10 points if yes).

___ TOTAL SCORE

0-24, D.B. Cooper (You can't be found, even after 20 years of an FBI manhunt)
25-49, Howard Hughes (You are extremely reclusive but you surface now and again in your own terms)
50-74, Brian Wilson (You are a fairly private person but make regular public appearances)
74-100, Lindsay Lohan (You are living in a fishbowl)

HOW TO VANISH CHALLENGE

How did you do? Maybe you are higher on the scale than you thought you would be, maybe not. Now for the challenge. The following tips are some of the most valuable and useful tips for protecting your privacy which cost only a little bit of time and no money. You can get started using all of them in just a few minutes. What a deal!

You will need to practice using some of them to become proficient, and you may not have a complete strategy yet for how to use them to your best advantage, but the earlier you start, the better it will be for you when you are ready to take your privacy protection to the next level. Just getting them all started will increase your privacy (and lower your score) significantly. The more people implementing best privacy practices results in an exponential increase in difficulty for those trying to breach privacy. So start implementing these best privacy practices just because you can!

1. GOOGLE VOICE

Google Voice is a free phone service, with a load of features, and significant privacy benefits. You are never required to give your name, never connected to any particular phone or location, and you can choose your number, forward your calls anywhere, and filter your calls efficiently. You can use Google Voice as a part of several

flexible strategies. One is to get a Google voice number to control the perception of where you live. You may choose any US area code. For example if you want to impress potential clients, you may wish to alter the appearance by having a New York City phone number. Get a New York Google voice number to give that impression.

Another strategy is to completely replace your old number with your new Google Voice number. Google Voice numbers are not listed and your name will not show up on any caller ID unless you have told them before that it is you. Your Gmail account is relatively anonymous and so your phone number can be relatively anonymous as well.

2. USE CASH

Transactional databases keep track of all kinds of information about average everyday purchases. The information in those databases is available to health insurance companies, creditors, law enforcement, marketers and others. Every time you transact with a card, you are tying yourself to that transaction. But I never buy anything remotely scandalous, how does it even matter if anyone knows what I buy?

Sally Harpold didn't think there was a problem either. She bought one box of Zyrtec for her husband and one box of Mucinex for her daughter in the same week. Both were bought over the counter, both regular, everyday purchases. Because she had to show ID to make the purchases, instead of giving another person cash to pay for it for her, she was identified in both transactions and the police were alerted of her purchase.[14] She was prosecuted on drug charges for buying too much ephedrine or pseudo-ephedrine based medicine within a one week period.

3. GET A FREE HUSHMAIL ACCOUNT

Most email is sent in its plain text form around the internet before it reaches its recipient. This is a lot like sending all of your regular mail by postcard. Everyone who handles the postcard, or every node that relays your emails around the Internet, can read the contents very easily. Hushmail is a service which sends encrypted emails for free. Encrypting emails protects the contents from being discovered.

For example, if you are sending emails to another Hushmail user, a court order from a court in British Columbia, Canada is the only way to get the emails from parties unwilling to disclose the contents. Even if you send emails to non-Hushmail users, the email can be password protected and provides other great security features that aren't present in most free email services. It is free to use and is as easy to use as Hotmail or other free email accounts.

[14] Indiana Code 35-48-4-14.7.

4. CLEAN UP ALL YOUR SOCIAL NETWORKING SITES

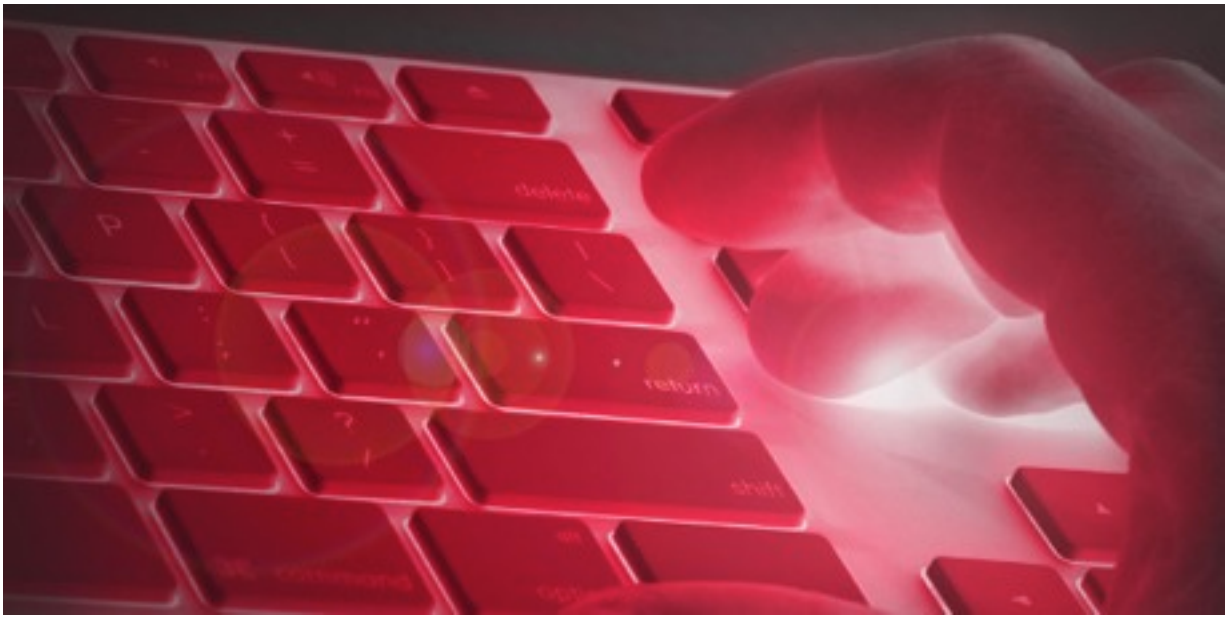
Facebook and other social networking sites are notorious for disregarding your privacy. Social networking, however, is a powerful tool that most people want to use. Make sure your privacy settings are as strong as they can be. If you have already submitted personal information to these sites, there is probably nothing you can do now to remove that information from their databases. You can, however remove it from your profile.

Take special care to remove incriminating information from your profile and from friends profiles. Nathalie Blanchard was denied benefits for her absence from work for severe depression because she was seen smiling in pictures on her Facebook profile. Who knows if she was faking the smiles or the insurance claim, but she was not obligated to disclose that information to her insurance company in the first place.

5. IMPROVE YOUR PASSWORDS

In any security system, the biggest weakness is often the password. There are actually computer programs that go through the dictionary and hundreds of thousands of other potential password combinations to unlock passwords. The more computing power the hackers have, the faster they can get in. The more complex the password the more difficult it will be to break, even with vast computing power. Use a combination of letters, numbers, symbols and punctuation, if possible. Make the passwords at least 8 characters long and preferably longer than 10 characters. This should keep your email and other password protected data from being hacked.

6. USE ENCRYPTION



Encryption is an underutilized tool many people can use to protect their privacy. One popular encryption program is True Crypt because it is extremely difficult to compromise. TrueCrypt-encrypted volumes are like normal disks. You provide the correct password (and/or keyfile) and mount (open) the TrueCrypt volume. When

you double click the icon of the file then the operating system launches the application associated with the file type and opens the file. Think of it like a USB drive or disk that no-one can access without your permission.

For example, you can create an encrypted volume and place within it a letter that contains a riddle in a regular text file, a treasure map to the trove of goods in PDF format and a few pictures of the spot in JPG or GIF format. When the volume is dismounted then it becomes encrypted and only the password will make the information coherent. The volume can then be sent via email, posted to a website, placed on a USB, etc. and because it is encrypted the information will not be compromised. One of the best parts about True Crypt is that it is completely free and open source. So visit TrueCrypt.org to get the latest copy for free.

CONCLUSION

When it comes to privacy there are many moving parts. If you can cause one of those parts to vanish then it will make it that much more difficult for a nefarious individual to harm you such as stalking you and compromise your personal safety, steal

your identity causing your financial problems, etc. These are some of the most simple but very effective things that you can do to protect your privacy.

The more people implementing best privacy practices results in an exponential increase in difficulty for those trying to breach privacy. So please share this free report with your friends, family and others you care about.

Once you have implemented these simple and free best practices then you are ready to go to the next level with the book How To Vanish and other products from HowToVanish.com that provide far more comprehensive, in depth and even more profitable strategies for protecting your privacy. If you are particularly savvy and willing to take the initiative then you may want a personal consultation for your specific situation.