THE ABEL LAW GROUP, PLLC

MIKE A. ABEL

ATTORNEY AT LAW*

Gilbert Office
1734 E. Boston St. Ste. 103
Gilbert, AZ 85295

PHONE: (480)-478-4515
FAX: (480)-624-5968
mike@abellawgroup.com

Chandler Office
1035 W. Queen Creek Rd. Ste. 101
Chandler, AZ 85248

*LL.M. International Taxation
Admitted in Arizona, Ohio and
South Carolina

HOW TO PROTECT YOUR IDENTITY PART TWO

You have been careful; you purchased your home in a layered LLC for privacy and even maintained a virtual office to protect your privacy. Now when someone searches the local real estate records they cannot find your name, address, or other personal information, you are now good right? Well maybe to the everyday person, the backyard sleuth, and those who rely on public records however, unless you take several other steps companies such as Lexis Nexis, Acxiom, Oracle, Spokeo, Intelius, and a slew of others will find you and disclose your personal information to anyone willing to pay for it. Where do they get this information as there is no record of your information on public record? Well, you should have been reading the privacy policies on all of the websites, businesses, and government agencies that they provided to you and now your personal information has just been clicked away. What are the most common ways your personal information is leaked, in no particular order?

1. Utilities – Whether you know it or not, when you sign up for service with your local power or gas company, providing them with your address, phone number and other personal information, they take all of that information and promptly sell it to data collection companies.

2. Insurance Companies – You provide so much information to insurance companies. Not only your name, address, and phone number, but your relationship, marital status, email address, and a plethora of other personal information, much of which is shared with their affiliates and sold to the highest bidder.

3. Social Media – One of the biggest culprits out there. If you have not figured it out yet, Facebook, Twitter, Instagram, Tik Tok, and all the other ones out there sell one product, YOU. You post pictures, they own them, all your likes, dislikes, and even the address you sent via their private messaging service belongs to them and they sell it to everyone who wants it. And that two-factor identification, how do you think they get your phone number? They tell you its for security of your account, and you bought it.

4. Financial Institutions – Surely you can trust your local bank with your address and phone number, right? Check out their privacy policy and more than likely you will be shocked. And your credit card company, yeah, they even let data brokers know everything you purchased with their card!

5. Voting Registration – I have seen more people have their address, phone number, and email address exposed through the voter registration process. Yes, we all want to vote but recognize, all states provide some type of disclosure of your name, address, age, phone numbers, party affiliations, and more. Some states do provide a way to opt out of some of the disclosures, but it can be limited.

6. Cell Phones, Cell Phones, and more Cell Phones – We all are guilty of it, we love our cell phones. We download all of these Apps and their user agreements require us to let them track and share our information with them. We also love the GPS services, as we can navigate the quickest routes using our phone. Why do you think most of these Apps are free? Well, it is because you are the product. They sell you and your information and Google is the biggest culprit. Up to 84% of its annual revenue comes from ads and most are targeted because they have all of your information. Oh, and when you click the "I Agree" button, many of them just got permission to copy your address book.

These are only a few of the many ways your private information is ripe for disclosure and there is no way, no matter how thorough you are, that you can keep all of your information private unless you liquidate everything, buy gold, and live alone in the woods, which really is not an option. What can you do to at least minimize your footprint? Well, that depends on how much money you have. If you are uber wealthy it is easier, you merely create a Family Office that oversees all of your day-to-day operation. It buys all of your homes, cars, makes all of your payments, sets up utilities, and never discloses your personal information to anyone. Even then however, when the paparazzi snaps a photo of them walking into their home or they sign up to vote, it sort of blows their cover.

Unfortunately, most of us are not uber wealthy so what can we do to at least minimize disclosure of our private information? Here are a few tips, assuming you have purchased your home into the proper privacy vehicle:

1. Obtain a virtual office or PO Box in the name of an LLC that does not link back to any of your addresses but instead links to the PO Box or virtual office address. This assumes of course that you have used the proper strategy in forming your LLC to make sure not to disclose its manager or members.

2. Appoint a friend or your attorney as a manager of the LLC and have them sign all documents and assist in processing forms whenever your name is at risk of disclosure.

3. Appoint a separate manager to obtain insurance on your LLCs (assuming you have them owned by your LLC) to cover the house, car, boat, or other assets you are holding in your private structure.

4. Open all utilities solely in the name of the LLC. If the utility company requires a personal guarantee, ask if they will accept a larger security deposit. If they require an individual, you will have to have someone agree to sign up on your behalf and offer their guarantee.

5. When dealing with any company, ask for their privacy policies and try to opt out of any disclosures they may make.

6. Obtain a prepaid cell phone to use as your phone number when dealing with companies that distribute your personal information. Many of these phones allow you to use a call forward feature so you would not have to carry around two phones as long as you do not call them back on your personal one. You can also buy prepaid credit cards any time you need to buy more minutes or renew the phone if needed. There are also some apps that you can work with to do the same thing however, many also sell their users' information, or their terms of use allows them access to your existing phone's data.

7. If you do want to use your own cell phone, at least turn all of the location services and tracking Apps off. Apple now requires all App developers to add a button for you to grant the App permission to track you, just tap no. I also like using a VPN and there are several web-based phone Apps that you can use without giving your full or correct name.

8. When obtaining any government issued ID's or registering to vote you have a good chance of making information you want private public. Some states do have new guidelines about the disclosure of your information and even some opt out programs, but you will have to check. If you have more than one home, you can always "sacrifice" one of them and use another as your address. You can check your state's guidelines at: Access To and Use Of Voter Registration Lists (ncsl.org) to find out more.

9. Register email addresses with DMAChoice.org. This is a service that some email marketers use to scrub their list of email addresses that opt out just like the Do Not Call List.

10. You can pay private companies to keep your information away from data brokers. Sites such as DeleteMe and PrivacyDuck are two examples of companies that will help keep your data private. These services aren't free, though, and could cost you hundreds of dollars a year.

11. You can contact data brokers directly to opt out of their information mining services. Finding these can be a challenge. You can start with sites such as Big Ass Data Broker Opt-Out List, created by journalist Yael Grauer, and StopDataMining.me.

12. If you are going to use social media or any other online service, make up some of the personal information you are providing. Personally, I have lived at the Whitehouse and am over 200 years old.

13. VPNs are also recommended as your IP address will be shielded unless the service sells the information they collect, which is what all free ones do.

14. Lock your Credit Reports. Most people do not know that you can put a lock on your credit report that prevents anyone form accessing your file without your permission. Whereas your credit report contains more information about you then almost any other source, it is something I advise my clients to do on a regular basis. Equifax and TransUnion provide a free service for locking your file, but Experian has yet to join the club. You can also join one of the number of credit monitoring services however, many of them may help you fight identity theft but many of them also sell your information.

The above list is just a few of the things you can do to try to take back your privacy. I wish I could say that the government is going to step in to help, but they are not. Just look at the present legislation being proposed. The current administration wants to force your bank to report any transaction that occurs in your account that is over $600, as well as all transaction if your account once your account has more than $600 in activity during the year! Another reason I try to pay cash for so many things.

In addition, this past year the US took one giant step forward in following Europe's lead and started a beneficial ownership registry. In the 2020 National Defense Authorization Act our lawmakers slipped in a provision that any company that has over $500,000 in government contracts and other conditions to disclose the beneficial owners of the company to the US Treasury. That is over 87% of all companies in the US. They say this information will be keep private however, when has something not leaked form the government?

What does all this mean, well, first do everything you can to protect your personal information. The more you do the better you will be, but you also have to realize that total anonymity is virtually impossible to todays tech savvy world. But remember, if you just do the basic things your personal information will be shielded from the vast majority of the public, it is only the 1-2% of people that spend money with a data harvesting website that will locate your personal information and for those people, well maybe consider getting your CCW if possible.

Mike