By Ron ZayasCEO, 360Civic
Online Privacy Expert



PROTECTING YOUR PRIVACY ONLINE

How To Identify, Protect and Remove Your Private Information From Websites



INTRODUCTION

By now, nearly everyone recognizes the importance of protecting his or her credit information, social security numbers and bank account numbers. You may work with a company that helps you protect that information, to hopefully avoid the headaches and financial losses that result from identity and credit card theft.

But what about other types of personal information, such as your home address, and the names of your family members? This information is freely available on the internet and resold by companies every day. Does it require protection as well?

Yes, it does.

When people can find your home information, the name of your spouse and where your children go to school, they have the ability to bring grievances directly to your home. For many of us, that can be a nuisance. For people in specific occupations, that nuisance can become life threatening.

This ebook was written to provide important and potentially lifesaving information on the following topics:

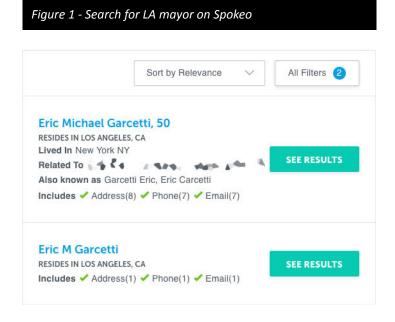
- 1. The dangers of having personal information available online where it comes from, how it gets there, and how it can be used in malicious ways.
- 2. The protections that exist for individuals and professionals (such as doctors, therapists, social workers, et al.), and the enhanced protection legally extended to judges, law enforcement officers, political figures and those in other select professions.
- 3. The options available for removing your information, from how to do-it-yourself to full-service removal and everything in between.



CHAPTER 1 — Your Private Information is Out There

Have you ever Googled your name? While it may be flattering to see how often you are cited on various websites, you may also notice that companies like Spokeo, BeenVerified and others run ads promising to provide more information about you, and that many other free sites already list your name and address. Spokeo is even nice enough to offer a list of your likely relatives (i.e., your spouse, children and parents).

To your right is a sample search on the mayor of Los Angeles, Eric Garcetti (we blocked out the names of his family for privacy, but his spouse and children are listed on the real result).



With a couple of clicks, virtually anyone can be found. If someone purchases the address information found above for Mayor Garcetti, and then enters it into Google maps, they can view a map to his house. Switch to the aerial view, and you can review the layout of the residence and surrounding grounds, including areas with limited visibility where a person could easily hide.

Further searches can identify local schools or with a little extra effort, the actual schools his children attend. Viewed in this context, a home address listed on a website becomes more ominous.





Where Does This Information Come From?

Most sites that sell this information point out that the information is publicly available. They buy DMV, property, court and other transaction records and simply compile it and make it more convenient to view. Most of the information does indeed come from different databases that are refreshed each month or on a regular basis. But the information is also combined with other sources that vary by site. Some use paid information from subscription sites and other sources to append your mobile phone number, the names of your relatives and even your photo. Getting a pilot's license, buying a home, declaring bankruptcy and other actions will get you on databases that show up online. Signing up for loyalty programs, giving your mobile phone to virtually any company and ordering free stuff can all increase the amount of information available about you online.

Even just providing your email to a company — for example, when you downloaded this ebook — may seem innocuous, but if you consistently use the same email address, it will get combined with other information you have entered and will get tied to your home address, phone number and more.

Editor's note: don't worry, 360Civic does not sell, barter or compile your information. The worst you will get from us is follow-up emails about our privacy protection service. Opt out if you wish, and your email is deleted forever.

The important thing to understand is that you do not opt in to having your information sold and bartered; these companies do it for profit without your consent.



How Do People Use This Information?

The ability to find anyone online makes it more convenient for employers to do a background check, or for a person to make sure that a prospective date is who he or she claims to be. Bill collectors also love this convenience.

But there are others who may also be very interested in finding you:

- 1. **Anyone you may have upset**, fired, ruled against, arrested or simply disagreed with over time. Police officers, judges and politicians have had their addresses collected and distributed online as part of doxing, protesting and intimidation attempts. Some have been targeted and killed at home.
- 2. **Ex-spouses, or old boyfriends and girlfriends**, whether you want them to find you or not, and that includes the abusive ones. Maybe someone isn't happy that you are dating his or her ex.
- 3. **People who don't agree with your political or religious views**, or even your stance on hygiene. The public health director for one of California's largest counties found protestors at her home after she said masks should be used to protect people during the pandemic. Ultimately, she resigned her job rather than be a public target.

Once purchased (assuming other free sources are not available), that information can be given out for free, put on social media sites and used for doxing and retaliatory efforts, not to mention posting on sites that actively target police officers, judges and public officials.

Even people in less visible professions — think therapists and social workers, or those that work in women's birth control clinics — may find themselves the object of unhealthy or unwanted attention, and thus may be targeted at home simply because someone disagrees with what they do.

Regardless of what compels someone to look for you, without taking action you have no control about whether or not they can find you.



What About Social Media?

A common argument used by people who don't believe we have a right to privacy is that much of this information is willingly shared on social media anyway. While that may or may not be true, there is a difference between someone choosing to share information, and having some company make that choice for them. As you will see from our later chapters, if you are sharing your phone number, address and family members on Facebook, LinkedIn or Instagram, you may want to stop. And you have the ability to do so. Unfortunately, getting companies that profit from selling your personal information to cease in their activities is more difficult, but it is possible and definitely worthwhile given the stakes involved.





CHAPTER 2 — What Protections Are Available

How easily you can remove private information depends in part on where you live and what you do for a living. Eventually, we hope laws will be passed that allow you to remove all of your information regardless of these variables, but today only some people have that ability.

Certain States Protect You More

California has the best privacy protection in the country. As a resident of California, you have the legal right in most cases to find your information and have it removed. If you live in other states, you have to depend more on the policies of the companies involved, but with enough determination you can be removed from their systems (click here to view a list of privacy laws in every state). Unfortunately, it may only last for a month or two at a time, since information tends to come back every time these sites reload their data.

People Who Protect and Serve Receive More Protection

If you are a police officer, court officer (e.g., judge, commissioner, attorney or executive in the employ of a court) or a publicly elected official, you have extra protections in states

like California, Nevada, Idaho, Utah, Colorado, Texas, Florida and New Jersey. In those states, in addition to the sites that sell your information, you can usually have your information removed from their underlying databases as well. Furthermore, states like California allow you to sue for assumed damages (at least \$4,000 per incident) when sites don't comply. And if you follow an exacting process, you can even appeal to your state's Attorney General's office for relief against incalcitrant sites. That is important, since even one site that carries your information is enough to thwart your protection efforts.

If you are in one of these categories — but don't live in these states — you can still get some protection, it just takes a little more work.

Everybody Else

If you have a job that doesn't afford access to greater protection, and/or if you are not a California resident, you can still protect yourself. But it takes a lot more work and diligence to achieve the same result. Nonetheless, the steps we outline in the next chapter can be effective.





CHAPTER 3 — Getting Rid of Information

There are four options for removing your information, depending on your circumstances:

1. **DIY** — Do it yourself. This works for everyone. It is time-consuming, but has the advantage of being free and making you painfully aware of how much information is out there. Just plan on devoting at least a couple of hours every week to keep this content off the Web. The steps on how to do so are covered in our next section.

Pros: Cheap. Only your time is involved, and you will likely do a comprehensive job of neutralizing threats. If you decide to go to court for civil actions, you can reap a windfall with companies that are not cooperating, assuming you live in certain states.

Cons: Time-consuming. You will likely need to devote at least two hours a week to search and removal efforts for each person you wish to safeguard.

2. Have your employer pay for it — Many organizations, from superior courts to police departments, from associations to unions, actually contract out this vital service for their employees at no cost, or offer attractive cost savings to members. If you are in one of the protected groups, or belong to an association or union, check with your benefits manager to see if they have something available. If so, you are fortunate and covered. Just sign up.

Pros: Generally free to you, or very low cost. Depending on the service selected, you can generally get a full-service program to handle searches and removals.

Cons: Not offered by every employer or association.



3. You Pay For a One-Time Service — One-time services charge an upfront fee of anywhere from \$50 to \$150 depending on how many people in your family you wish to protect. For that fee, you receive a prepared kit that opts you out of the major info selling services. You sign the letters they provide, and either mail them or pay to have the company do it for you. Most of these services also offer a "maintenance" search once a year or so, to see if any new information on you pops up.

These services are convenient, and are definitely better than not doing anything. However, they don't cover all the sites where your information will appear, and they don't follow up, so if a site does not remove your information, you may not know it. If someone can find your address online, it doesn't matter if it was on one of the services they covered, or from a different source. They still have your address, and the harm is done. When items from search results are removed, other (equally damaging) items move up in their place. This leads to a false sense of security, especially since many sites are notorious for re-adding your information after you have opted out.

Reviewing your information once a year is not helpful. Because items can reappear, regular monitoring (at least weekly) by you or by a service needs to happen, or your protection is illusory. The practical difference between finding your address on two sites or 40 sites is irrelevant. If the information can be found with one simple search, your security is compromised.

Pros: Easy to implement, affordable for most and does a good job of removing many threats.

Cons: Only covers protected occupations in certain states, does not remove all threats, and only offers yearly monitoring at an additional charge.

4. You Pay for an Ongoing Subscription — (Full Disclosure: 360Civic provides this type of service) This type of service, also called a full-service or concierge-type service, searches the internet on a regular basis (generally daily or weekly), identifies when a match is found and initiates the removal process for you. If the item is not removed, the service follows up and escalates the issue until it is removed. If a company is unwilling to remove the information after multiple attempts, the issue is escalated to the State Attorney General's office, or a complete record of requests is generated so you can initiate a claim in small claims court (if your state allows civil recovery). A personalized portal generally fills you in on every instance found and removed, and provides detailed information for every action taken on your behalf.

In this manner, you are constantly being protected, with a combination of automated systems and real-life people. These types of subscription services range from \$8-\$15 a month, depending on whether you are protecting yourself or your entire family, with discounts available for paying yearly instead of monthly. You can view or sign up for the IronWall360 full-service removal product here.

Pros: Aside from DIY, the only comprehensive way to remove your information. Constant monitoring and full service means you are protected constantly.

Cons: There is a monthly fee that averages around \$8 a month.



The chart below compares the three non-employer paid options.

Protection Services Options			
	DIY	One Time Service	Full Service Subscription Service
Can remove information	✓	√	\checkmark
Will remove all information	✓	×	✓
Provide regular monitoring	✓	×	
Escalate issues	✓	×	✓
Keep notes for lawsuits	✓	×	✓
Are available to the general public	✓	×	
Portal with all searches & removals?	×	×	
Cost	Time	\$50 – \$150 one time	\$8 – \$10 a month (\$80 – 120 a year)

Figure 2 - Removal service options

Whichever option is right for you is likely determined by your budget, whether you are in a protected class and where you live. But for most people, unless the protection is available through an employer or association, the best option will be either DIY or a subscription service.

If you decide to remove your information yourself, the next section provides the information you'll need to accomplish this.



Removing Your Information — Do It Yourself

Removing your personal information from the internet involves four steps:

- 1. Identifying your options and legal protections: this is based on where you live and whether you are in a protected profession, as discussed earlier. All is not lost if you do not live in California, or if you are not in law enforcement, a court officer or an elected, public official, but you will have to work a little harder to achieve results.
- 2. **Run a search:** You can't identify what information is out there until you run a search. You will also need to run your name on the sites we list in the appendix, since they may not come up in just a standard search engine query. Remember, the threat is not your name being listed, but your name and address, so concentrate on those.
- 3. **Start the removal process:** Once you know where your information appears, it's time to start opting out. How you do so once again depends on whether or not you are in a protected class.
- 4. **Develop a search schedule:** New companies come into existence every day, and existing companies that removed your information will often refresh their databases and re-add you in. A weekly search pattern helps you identify threats.

Each of these steps is defined and explained in detail below.

Step 1 — **Identifying Your Legal Options**

What you can remove, how long it should stay removed, and what you can do if a website will not comply is based on where you live and what you do for a living.

1. If you live in California, regardless of your profession, you are protected by the California Consumer Privacy Act (CCPA). The CCPA allows you to view any information stored on you, mandates that a company explain what they do with the information and allows you to have the information deleted without prejudice or penalty. Companies can be fined for not adhering to the law, and will go out of their way to say they don't "sell" your information. But they will barter it for compilers who do sell it. Either way, if your information is there, and you live in California, you can have your information removed.

What is important here is where you live, not where the website is located. Your California protections follow you throughout sites located in all 50 states. The only challenge may be finding the reference to CCPA on a website, as it is often buried on a page few visitors access.



California requirements

The California Consumer Privacy Act (CCPA) requires specific disclosures for California residents.

This Privacy Policy is designed to help you understand how Google handles your information:

- We explain the categories of information Google collects and the sources of that information in Information Google collects.
- · We explain how Google uses information in Why Google collects data.
- We explain when Google may share information in Sharing your information. Google does not sell your personal
 information.

The CCPA also provides the right to request information about how Google collects, uses, and discloses your personal information. And it gives you the right to access your information and request that Google delete that information. Finally, the CCPA provides the right to not be discriminated against for exercising your privacy rights.

We describe the choices you have to manage your privacy and data across Google's services in Your privacy controls. You can exercise your rights by using these controls, which allow you to access, review, update and delete your information, as well as export and download 2 a copy of it. When you use them, we'll validate your request by verifying that you're signed in to your Google Account. If you have questions or requests related to your rights under the CCPA, you (or your authorized agent) can also contact Google 2.

The CCPA requires a description of data practices using specific categories. This table uses these categories to organize the information in this Privacy Policy.

Here is an image of the relevant CCPA section from Google, as an example of how sites have to treat California residents:

Cons: There is a monthly fee that averages around \$8 a month.

2. If you are a law enforcement officer, court officer (judge, executive, attorney working for the court), or elected public official, and you live in California, Nevada, Idaho, Utah, Colorado, Texas, Florida or New Jersey, you have even more protections and remedies. The sites have to remove your information (with very few exceptions for federal government sites) and if they refuse (as some will), you can sue. In California, sites must remove your information for four years. If they don't, you can sue them in small claims court and recover up to \$4,000 per incident. This can be lucrative when you find sites that just don't get it, and many don't. You can also appeal directly to your state's Attorney General's office and file a complaint. If you kept good records of when and whom you contacted, these offices will likely be helpful. Otherwise, sites may just respond with "we never received the removal request but will comply now".

If you are in these protected occupations and you don't live in one of these states, you still have some protections, which we will discuss in the removal section.

3. For everybody else, you have to rely on the opt-out process for each website. Daunting, but not insurmountable. Just remember what is at stake here.



Step 2 — Run a Search

Generally, you want to remove anything that has your name and address. Start with a search on Google, and then conduct one on Bing. They will have similar but not exact results, so make certain you retrieve a large cross section of information.

Because your address is the most potentially damaging data, try searching for that first. Here is a sample search based on an address in Texas. Start with your street name and city first, for example "909 Rover Pass, Cedar Park."

Figure 4 - Search results (address & name redacted) https://blockshopper.com > cedar-park > property > 90... : | 909 | Pass, Cedar Park, TX 78613 , 909 Cedar Park, TX 78613 Find homes for sale, market statistics, foreclosures, property taxes, real estate news, agent ... https://app.listingspark.com > real-estate > texas > 909-d... Cedar Park, TX 78613 | ListingSpark . Cedar Park, TX 78613. Unlock Price. 3 Beds; 2 Baths; 1,530 Sq.Ft. 1993 Year Built. Add to favorites Hide from search results ... https://www.austintexasrealestate.com > listing > 12976... Cedar Park, TX 78613 - Gene Arant Team The property located at 909 Cedar Park, TX 78613 is a House property. Built in 1993, the property at 909 Dover Pass is 1 story, has 3 bedrooms, ... https://www.zillow.com > Texas > Cedar Park > 78613 909 Deer Grove Dr, Cedar Park, TX 78613 | Zillow The property 909 Deer Grove Dr, Cedar Park, TX 78613 is currently not for sale on Zillow. View details, sales history and Zestimate data for this property on ... https://www.zillow.com > Texas > Cedar Park > 78613 909 Canyon Springs Dr, Cedar Park, TX 78613 | Zillow 909 Canyon Springs Dr., Cedar Park, TX 78613-1666 is currently not for sale. The 3547 sq. ft. single-family home is a 5 bed, 4.0 bath property. This home was ... Parking: Garage - Attached Missing: dever | Must include: dover



While most of the listings have an address, they have no names attached to them, which is acceptable. But the first listing clearly includes the address and the names of the owner (blocked out of the image). This is the result you want to focus on.

Click on the link, and then copy the name of the site and the URL to your tracking spreadsheet. It may help to capture all offending sites first on the spreadsheet, and then go back for removal later. That way, you will get better at removing sites as you proceed.

Search through at least the first ten pages of search results, or until you begin to see the results peter out or change to other addresses (such as you see towards the end of the page in Figure 4). Repeat the search in Bing.

Then try searching for your name and city to return a wider range of results. This will also bring up most of the paid sites that tend to list people that way. Add any positive results into your spreadsheet.

Searching Paid Sites

Searching paid sites is a little different than standard search engine searches, although many of these sites will appear with your initial search. In the example shown above, you may have to search the specific sites referenced in the appendix to ensure your name is removed.

Take any one of the paid sites and enter your name and city and see what happens. As an example, we did a search for Robert Styles, who we know lives in North Carolina and is in his midthirties. Results from paid sites appear similar to the one in Figure 5.

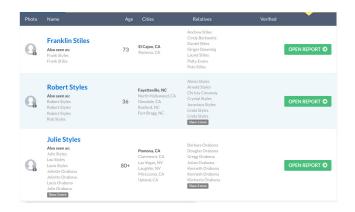


Figure 5 - Typical paid site result

As you can see, my target appears along with the names of his family (likely spouse and children). If I click on the "Open Report" link, I can give my credit card and get more detailed information on Robert, including his address, phone, past addresses and relatives. It is that simple to find someone, and for someone to find you. Click on the link and copy and paste the URL of the edited report (they won't show you the full report until you pay for it, and you needn't do that to have it removed) into your spreadsheet.

Repeat this for the 40+ paid sites that most commonly have your information. New sites appear all the time, so if you notice one in the ad section of your search engine searches, add them to your list.

Once your spreadsheet is completed, you are ready to begin the removal process.



Removing Your Personal Information

This is where you finally start to see results. While every site is slightly different in how to opt out, the relative steps are the same. We will use Spokeo, a popular website for information, as an example.



Figure 6 - Your profile link on Spokeo



Figure 7 - Look for the Privacy or Opt-Out Link at the bottom of the page

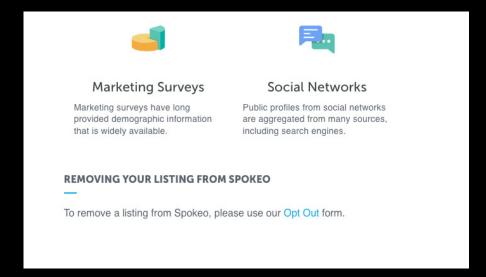
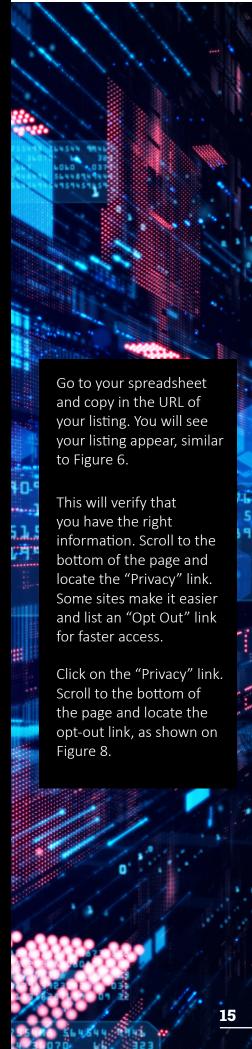


Figure 8 - Opt Out link in Spokeo





The opt-out link takes you to a simple form where you enter the URL that you copied onto your spreadsheet, add your email, complete the ReCAPTCHA and then follow the process. They will send you an email where you confirm your information. Figure 9 shows a completed form.

Removing Your Listing from Spokeo Spokeo aggregates publicly available information from third party sources. Therefore, removing a listing from our directory will not remove your information from its original source and therefore your information might still appear on other directory sites. You may have multiple listings on Spokeo, each of which is identified by a unique URL and must be removed individually. Also, since we continually receive new and updated records, please regularly check Spokeo for additional listings that may appear. To remove a listing from Spokeo, please enter the URL of the profile and your email address (for verification purposes) URL Profile URL Example: "https://www.spokeo.com/Smith-Sample/Houston/TX/p12345678" Payment URL Example: "https://www.spokeo.com/purchase?q=Smith%20Sample#Sample:12345678" s://www.spokeo.com //California/Mission-Viejo/p2017110408247322172297377478599 Email Address To complete this process we will send you a confirmation link junk@myemall.com Pim not a robot Figure 9 - A completed Spokeo removal form

Note: This is where the process is different if you are from California, or are in a protected class. Rather than complete the opt-out process, click on the chat box or call the phone number (we recommend the chat box so you have a record of the information) and specify that you are either a California resident protected by CCPA, or you are a judge, law enforcement officer, or elected official in any of the states listed with statutes, and you need to be removed under this protection. A simple prepared statement like:

"California Public Records Act Authorized Request (California Government Code 6254.21)

Please be advised that I am formally requesting that your website immediately cease and desist from publicly posting or publicly displaying on the internet my home address and/or telephone number. You are required by law to comply with this request, as I am a resident of California, and/or serve in one of the professions that are afforded additional privacy protection, so I may safely perform my job. Removal of this content is required for a period of not less than four years."

The person on the chat should make the removal request while you are online, and give you a confirmation. Copy and paste the information from the chat box into your spreadsheet along with the date. This will come in handy if you ever need to sue or file a complaint.



Repeat as Often as Necessary

Complete this process for each one of the paid and non-paid sites where your name appears. If the site does not have a chat box, use the email address provided to send your information, and keep track of the results. It is important so you can refer to this if your personal information is not removed, or for when your name invariably reappears.

Sites That Won't Remove Your Information

There are some sites that are not bound by state statutes, or even privacy laws like CCPA. These include federal government sites, state licensure sites (e.g., the State Bar, or where licenses are obtained for marriage and family therapists, cosmetologists and the like) county property assessment sites and even court information. But there are strategies to deal with these sites as well:

- 1. **License sites:** If you have a license (e.g., a pilot's license, license to practice medicine or law) you can change your address on the site to one for a mail forwarder, or consider using your office address instead of your home address (after all, your work address is likely already public). It is not illegal to do so, as long as you provide a valid address where you can receive mail.
- 2. **County property listings:** If you are in a protected profession or even just a sensitive one contact your county assessor's office and ask to have your name redacted from public records. Clearly state why you are making the request, state the statute if available, but make a compelling request for why your name need not appear. This often works. If you need assistance, email us at ironwall360@360civic.com and we will provide you sample language that has worked for us.

You can also move your home into a trust, thereby removing your name as one of the owners.

3. **Social media sites:** Social media sites don't have to remove your information since you provided it freely. Luckily, you can change it on your own. Never post your address (or allow your children to) on social media sites. And don't provide your mobile phone or post it anywhere. This is one of the simplest ways for companies to find you. Seriously, do not give your mobile number to anyone. Either get a cheap VOIP number and forward it to your cell phone, or just stop giving people your mobile number. If it is required on a form, put in 555-1212. Mobile numbers are worth a lot of money to marketers and they will resell them often. Just don't do it.

Dealing with these sites will eliminate any holes in your protection. If you find other sites that will not remove your address, let us know at <u>ironwall360@360civic.com</u> and we can help devise a strategy to remove the information.





CONCLUSION

It is difficult and time-consuming to remove your information from the Web. You shouldn't have to do this, but it is the situation we are in, and for many people the risk of having a home address appear on a website is just too great. This eBook gives you the steps to take control of your information. If you still don't have the time or energy to do it yourself, we hope you will consider IronWall360 from 360Civic. You can try the service with no risk for 60 days, and if you decide to continue you will pay just pennies a day to protect you and your entire family.

More information is available at 360civic.com/blueprotect.



Appendix

Pay sites you should search that sell your information:

411 Locate

555-1212

Abacus

Acxiom Corporation

Addresses.com

Advance Background Checks

Ancestry

AnyWho

BeenVerified

<u>BlockShopper</u>

Confi-Chek

Cyber Background Checks

Data Axle USA

DOBsearch

Haines Criss+Cross

Instant Checkmate

Instant People Finder

<u>Intelius</u>

Lexis-Nexis

LocatePLUS, Inc

MyLife

<u>PeekYou</u>

<u>PeopleSmart</u>

PIPL

Private Eye

<u>PublicRecords</u>

Radaris America

Spokeo

Suarez Corporation Industries

<u>TransUnion</u>

<u>US Search</u>

Westlaw

White Pages

Zaba Search



