
# Managing Your Online Presence

Jared Dearing
Mike Garcia

Release 1.0

# CONTENTS

CHAPTER

# ONE

# MANAGING YOUR ONLINE PRESENCE

Everyone has an online presence. Some aspects are largely out of your control, but many can be managed directly by you, such as your social media accounts. You can indirectly control other information, like how you appear–or don't–in people finders.

Election officials and other election workers are attractive targets for cyber-attacks and social engineering attempts. By implementing the recommendations outlined in this document, officials can mitigate risks, protect their personal information, and secure the privacy of themselves, their family members, their staff, and their organizations.

This guide provides actions to manage your online presence. From separating personal and official social media accounts, removing personal information from the web, and using privacy settings effectively, the guide supports election officials' security and privacy.

Read on for guidance on managing your online presence. You can download the quick guide below for a one-page summary of this guide.

CIS Center for Internet Security® | Creating Confidence in the Connected World.™

# How to Secure Social Media Accounts

### Enable Two-Factor Authentication (2FA)

Use methods like SMS verification, authenticator apps, or hardware security keys to add an extra layer of security to your social media accounts.

### Use Strong, Unique Passwords

Use long passphrases that are hard to guess and avoid personal information. Consider using a password manager for generating and storing complex passwords securely.

### Be Wary of Phishing Attempts

Exercise caution with messages and friend requests. Verify the authenticity of messages that ask for personal information, and be skeptical of urgent or manipulative language.

### Regularly Update Your Software

Ensure all social media apps, operating systems, and web browsers are up to date to protect against security vulnerabilities.

### Use Secure Networks

Avoid using public Wi-Fi for sensitive transactions. Use VPNs for enhanced security when accessing social media accounts on public networks.

### Monitor Account Activity

Regularly check login history and account activity for unauthorized access. Set up notifications for unrecognized logins.

# Tips to Enhance Social Media Privacy

### Private vs. Public Accounts

Maintain private settings on personal accounts to protect information. Use official accounts for public communications, keeping them professional and transparent.

### Control Over Content Sharing

Private accounts allow for better control over who can interact with your account and view your content, reducing the risk of your account being inadvertently associated with misinformation.

### Avoid Conflicts of Interest

Keep personal opinions and professional responsibilities separate to preserve impartiality and public trust.

### Operational Security

Protect against social engineering and other attacks by limiting exposed information, including by disabling location services, removing locations from photos and posts.

### Preserving Public Trust

Demonstrate commitment to privacy and security, building confidence in the electoral process and reducing misinformation.

### Engage with Family on Privacy

Discuss the importance of digital privacy with family members to protect personal information from being exploited.

# How to Reduce Your Digital Footprint

### Delete Unnecessary Accounts

Regularly review and delete old or unnecessary social media accounts to minimize your online presence.

### Limit Exposure

Turn off tagging and review posts where you're tagged. Control the visibility of your posts and personal information.

### Remove Real Estate Information

Request that real estate and rental websites remove photos and information about your personal addresses.

### Blur Photos on Mapping Apps

Request blurring of photos of your personal residence from mapping apps.

CHAPTER

TWO

# SOCIAL MEDIA SECURITY

Securing social media accounts is crucial to protect personal information, prevent unauthorized access, and safeguard against potential cyber threats. For election officials and their staffs, enhancing the security of social media accounts is not just a matter of personal privacy but also a critical component of safeguarding the integrity of your election systems. Election officials are increasingly targeted by malicious actors aimed at undermining election infrastructure and public trust in the democratic process. Election offices can significantly reduce risk by encouraging, or, where appropriate, requiring, these best practices by all who work in election administration can.

These recommendations are valid for personal accounts as well as official election office accounts.

## How to Secure Social Media Accounts

### Enable Two-Factor Authentication (2FA)

Use methods like SMS verification, authenticator apps, or hardware security keys to add an extra layer of security to your social media accounts.

### Use Strong, Unique Passwords

Use long passphrases that are hard to guess and avoid personal information. Consider using a password manager for generating and storing complex passwords securely.

### Be Wary of Phishing Attempts

Exercise caution with messages and friend requests. Verify the authenticity of messages that ask for personal information, and be skeptical of urgent or manipulative language.

### Regularly Update Your Software

Ensure all social media apps, operating systems, and web browsers are up to date to protect against security vulnerabilities.

### Use Secure Networks

Avoid using public Wi-Fi for sensitive transactions. Use VPNs for enhanced security when accessing social media accounts on public networks.

### Monitor Account Activity

Regularly check login history and account activity for unauthorized access. Set up notifications for unrecognized logins.

## 2.1 Enable Two-Factor Authentication (2FA)

Two-factor Authentication (2FA), or Multi-Factor Authentication (MxFA), enhances the security of your social media accounts by requiring two or more authentication factors to log in, which significantly reduces the risk of unauthorized access. Multiple authentication factors mean at least two of the following: (1) a password, (2) something you have like a hardware device, and (3) something you are like facial recognition or a fingerprint. While all types of MFA have vulnerabilities, any types is better than using a password alone.

### 2.1.1 Common Types of MFA

- **SMS-Based Verification**: This method sends a text message with a unique code to a mobile phone, which you must enter in addition to your password when logging in. Despite its convenience, SMS-based verification can be vulnerable to phishing and SIM swapping attacks.
- **Authenticator Apps**: Authenticator apps such as Google Authenticator or Okta generate a temporary code that refreshes periodically. You enter this code along with your password when logging in. This is sometimes implemented as a push notification on your phone asking you to confirm you are trying to log in. This method is more secure than SMS because it is tied to your device and not just the cellular carrier's records of your SIM card.
- **Hardware Security Keys**: These are physical devices that communicate with the device you're using to log in (usually a phone or laptop) either by plugging it in or through NFC (the same technology behind tap-to-pay for credit cards). They are considered a highly secure form of MFA as the key must be physically present to gain access.

### 2.1.2 Implementing MFA on Social Media Platforms

Set up MFA: Facebook[1] | X (formerly Twitter)[2] | Instagram[3] | TikTok[4] | LinkedIn[5]

## 2.2 Use Strong Unique Passwords

Old recommendations for passphrases required complexity and composition rules like using uppercase and lowercase letters, numbers, and symbols. More recent research[6] has found that longer passwords are more secure and easier to remember than complex ones. Reusing passwords across accounts creates the risk that if one is compromised, all your accounts could be compromised. So, use long passphrases and make passwords unique, especially for the accounts that are most important to you.

[1] https://www.facebook.com/help/148233965247823
[2] https://help.x.com/en/managing-your-account/two-factor-authentication
[3] https://help.instagram.com/566810106808145
[4] https://support.tiktok.com/en/safety-hc/account-and-user-safety/account-safety
[5] https://www.linkedin.com/help/linkedin/answer/a1354987
[6] https://www.nist.gov/blogs/taking-measure/easy-ways-build-better-p5w0rd

- **Memorability and Length Over Complexity**: A longer password that consists of simple, easy-to-remember words or phrases (often referred to as a passphrase) can be more secure than a shorter, complex password. For example, a passphrase like "3 blue jays sing morning chatter" is both easier to remember and harder to crack than a complex shorter password like "B$1uC@f3!". (Use spaces between words when permissible.) Older systems sometimes still require complexity—and might even limit how long a password can be—but wherever possible, use passphrases instead.
- **Avoid Personal or Commonly Used Phrases**: When creating a passphrase, pick a string of words that are not a common phrase or easily associated with you. Avoid using personal and easily guessed information such as birthdays, names, sports teams, pets' and children's names, hobbies, song lyrics, or famous quotes. Do not use easily guessable passwords like "password", "123456", or "qwerty". Visualization is often the easiest way to do this. Try choosing a handful of items from your living room or office (e.g., Yellow Note Pad Blue Pen Apple Laptop). It'll be easy to remember but effectively impossible for someone to guess.
- **Consider Using a Password Manager**: Keeping strong, unique passphrases for each of your accounts presents a real challenge. A password manager solves this problem by securely storing all your passwords in an encrypted format and allowing you to access them in a secure way such as with facial recognition on your phone. Password managers will create strong passwords for you and keep you from reusing passwords across multiple sites. They also protect against phishing because they will only present a password to the same site on which you created it. For added convenience, many password managers allow you to securely sync your passwords across devices. If you don't use a password manager in your office, work with your IT team to implement this best practice—it's a lot better than keeping them on a sticky note!

## 2.3 Be Wary of Social Media Phishing Attempts

Social media platforms are prime targets for phishing attacks due to the vast amount of personal information available and the high level of trust users place in their connections. Easily accessible personal information can aid bad actors in generating spear-phishing attacks against you or your contacts. Below are several concepts to keep in mind when defending against social media phishing attacks.

- **Beware of Suspicious Messages**: The most critical step in protecting your social media accounts is to be wary of suspicious messages and direct messages, including friend requests. Cybercriminals often create fake profiles or use a previously hacked account to extract personal information, payment information, or login credentials. Always verify the authenticity of messages that ask for personal information or direct you to log in to another site, even if they seem to come from a friend.
- **Be Cautious of Urgency**: Phishing attempts on social media often use urgent and manipulative language to trick users into acting hastily. Be skeptical of messages that create a sense of urgency, such as warnings that your account will be closed unless you take immediate action or offers that seem too good to be true. This tactic is designed to prey on emotions and should be a red flag.
- **Examine the Sender's Profile for Authenticity**: Before interacting with a user, one you

haven't interacted with before, examine the sender's profile for signs of authenticity. A new account with minimal activity, few friends, or missing profile details can be a sign of a fake account created for phishing purposes. Also, be cautious of duplicate friend requests from people you are already connected with; this could indicate that the second account is an imposter.

- **Threats from Generative AI**: Generative AI enables the creation of highly realistic fake images, videos, and profiles that can easily deceive users to do a more convincing job of all the threats above. Stay informed about the capabilities of generative AI and be extra cautious with content that seems unusually sophisticated or too personalized. AI-generated phishing will still use many of the same techniques as traditional phishing, including urgency of action, offers that are too good to be true, and suspicious or slightly altered account names. Use the same tools you would use in avoiding traditional phishing attacks: be suspicious and cautious and verify the authenticity of messages, links, and attachments before interacting with them.

## 2.4 Secure Your Email Account

Securing your email account is a fundamental step in protecting your online identity given its interconnectedness with various social media platforms. The recommendations listed elsewhere in this document, such as using passphrases and implementing 2FA, are also effective for securing your email account.

The security of your email account is integral to your online safety. By following the steps in this document, you can reduce the risk of account compromise and protect your personal information.

## 2.5 Regularly (or Automatically) Update Your Software

Update the apps you've installed, as well as the underlying operating systems and browsers for your devices. Most devices allow for automatic updates.

### 2.5.1 How to Set Automatic Updates on iOS

1. Open Settings: Start by tapping the Settings icon on your iOS device.
2. Navigate to General: Scroll down and select the "General" option.
3. Software Update: Tap on "Software Update" to enter the update settings.
4. Automatic Updates: Here you will see an option for "Automatic Updates". Tap into it.
5. Enable Updates: You will find two options—"Download iOS Updates" and "Install iOS Updates". Toggle both to the ON position. This will allow your device to automatically download and install updates when they are available.

### 2.5.2 How to Set Automatic Updates on Android

1. Open the Google Play Store: Start by opening the Google Play Store app on your Android device.
2. Access the Menu: Tap on the menu icon (three horizontal lines), then select “Settings”.
3. Tap on Auto-update apps: Under the “General” section, find and tap on “Auto-update apps”.
4. Select an Option: You can choose to auto-update apps at any time or only over Wi-Fi to avoid using data. This ensures that not only your apps but also the operating system receives updates as they are rolled out by app developers and Google.

By following these steps, you can ensure your apps on both iOS and Android devices are always up to date, keeping your device secure and enjoying the latest features and improvements.

## 2.6 Use Secure Networks

Avoid logging into your social media accounts on public Wi-Fi networks.

### 2.6.1 Understand the Risks of Public Wi-Fi

- **Unencrypted Networks**: Many public Wi-Fi networks do not encrypt the data being transmitted over them. This means that anyone else on the network could potentially intercept the data you send and receive, including your social media passwords and personal messages.
- **Man-in-the-Middle Attacks**: Attackers can position themselves between you and the connection point. Instead of communicating directly with the hotspot, you’re sending your information to the attacker, who then relays it on to your intended destination—but not before they make a copy for themselves.
- **Malicious Hotspots**: Some attackers set up Wi-Fi connections with legitimate-sounding names to trick users into connecting. Once connected, the attacker can attempt to infect your device with malware or monitor your internet activity.

### 2.6.2 Use VPNs for Enhanced Security

- **Encryption**: A VPN encrypts your internet traffic, which means that even if someone were able to intercept your data, they would not be able to easily read it. This encryption helps protect your personal information and login credentials.
- **Choosing a VPN**: It’s important to choose a reputable VPN service. Look for VPNs that have a strong privacy policy, do not keep logs of your activity, and offer high-speed connections. Some well-regarded VPN providers include options that are paid as well as some limited free services.

### 2.6.3 Best Practices for Using Secure Networks

- **Use Mobile Data When in Doubt**: If a secure Wi-Fi network is not available and you must access sensitive accounts, consider using your mobile data instead. Mobile data connections are generally more secure than public Wi-Fi. You may need to change your cellular plan to use your phone as a hotspot.
- **Avoid Public Wi-Fi for Sensitive Transactions**: Always avoid using public Wi-Fi for accessing email or conducting any sensitive transactions.
- **HTTPS**: Ensure the websites you visit are using HTTPS, which indicates the data sent and received is encrypted. Many browsers have a lock icon to signify an encrypted connection.

## 2.7 Monitor Account Activity

Regularly monitor your login history and account activity. Many social media platforms provide tools that let you see where and when your account has been accessed.

View your activity logs: Facebook[7] | X[8] | Instagram[9] | TikTok[10] | LinkedIn[11]

You can also determine if your passwords, email, or personal data has been revealed in various data breaches. HaveIBeenPwned.com[12] collects and analyzes hundreds of database dumps and posts containing information about billions of leaked accounts. You can also set up a notification service to be informed about future breaches.

[7] https://www.facebook.com/help/289066827791446
[8] https://help.x.com/en/managing-your-account/using-the-post-activity-dashboard
[9] https://help.instagram.com/460411108811350
[10] https://support.tiktok.com/en/account-and-privacy/account-privacy-settings/activity-status-on-tiktok
[11] https://www.linkedin.com/help/linkedin/answer/a1341842/view-your-activity-and-data-on-linkedin?lang=en
[12] https://HaveIBeenPwned.com

CHAPTER

# THREE

# SOCIAL MEDIA PRIVACY

To effectively serve voters, election officials must engage the community, which effectively requires a social media presence. This guide offers strategies for protecting personal data, delineating personal from professional online identities, and implementing digital security.


## 3.1 Personal Social Media Accounts Versus Professional Accounts

Your personal social media accounts and your professional or official accounts serve different purposes, and your official accounts likely have distinct guidelines and expectations.

- **Create Clear Boundaries between your Personal and Work Accounts**: Your personal accounts are your private spaces to share life updates, express your opinions, and connect with friends and family. In contrast, your official account or accounts as an election administrator are public platforms created to share information, updates, and communications relevant to the electoral process. You should carefully curate content to reflect the objectives and values

of your official role, clearly separating personal opinions. This approach helps balance your private and public lives, ensuring your personal social media use does not affect the perceived integrity and impartiality crucial to your duties.

- **Avoid Accidentally Posting on the Wrong Account**: Segment your personal and professional social media accounts and, when possible, use different devices for each. Avoid accessing personal social media accounts with government assets, including work computers and government-issued mobile devices. Unfortunately, it's all too common to see public officials who have personal and work-related accounts post or like something, thinking they were using their personal account when they posted to their professional account. These types of mistakes can cause irreparable damage to both your individual reputation and the reputation of the election jurisdiction that you govern.
- **Be Vigilant on All Accounts**: Malicious actors will often target the personal accounts of public officials, hoping you will be less vigilant there. Whether you are managing a work or personal account, you should always be suspicious of clicking links and attachments from unknown and untrusted sources.

## 3.2 Lower Risks by Using Private Accounts

While social media platforms allow for efficient communication and engagement with the public, they also expose officials to potential security vulnerabilities. Malicious actors exploiting your publicly shared personal information can lead to doxxing, identity theft, phishing (of you or by someone pretending to be you), and direct threats to you and your family's safety.

While official accounts likely need to be public, keeping your personal accounts private and controlling who you allow to follow your accounts can significantly mitigate these risks, ensuring that sensitive information is shared only with a trusted circle. This will help you control who can view your posts and reduce your exposure to harassment, particularly during heated election periods. These methods can limit unwelcome interactions and messages from potentially malicious individuals. For those facing directed and/or extreme harassment, consider temporarily pausing or deactivating personal social media profiles as a measure to reduce unwanted interaction and information leakage.

## 3.3 Review and Remove Followers on Personal Accounts

Regularly review and remove followers on your personal social media accounts, particularly if your role involves increased risks to personal safety. Limit followers to those in your immediate circle to keep personal information private. As your network grows, managing information security becomes more complex. By restricting your circle to trusted contacts, you significantly lower the chance of personal information being misused. This focused strategy enhances both your privacy and your information security, serving as a wise measure to protect your digital presence.

## 3.4 Privacy Settings on Social Media Platforms

Accessing the privacy settings on various social media platforms is crucial for managing what information is visible to others and for controlling your online experience. The exact steps may vary slightly depending on whether you are using a web browser or a mobile app, and the platforms themselves may update their interfaces and options over time.

Adjust your privacy settings: Facebook[13] | X[14] | Instagram[15] | LinkedIn[16] | TikTok[17]

## 3.5 Control Who Can Tag or Mention You on Social Media Platforms

Controlling who can tag or mention you on social media platforms is essential for maintaining online privacy and managing your digital footprint. It gives you control over the content associated with your profile and helps prevent unwanted attention or harassment.

Manage who can tag you: Facebook[18] | X[19] | Instagram[20] | TikTok[21]

## 3.6 Disable Location Services

Turn off location services for social media apps to prevent your location from being shared when you don't want it to be.

Apple iPhones:

1. Go to the Settings app.
2. Tap on Privacy.
3. Tap on Location Services.
4. To turn off location services for all apps, toggle 'off" next to "Location Services".
5. To turn off location services for specific apps, scroll down and select the app, then choose "Never" or "While Using" instead of "Always."

Android Phones:

1. Open the Settings app.
2. Tap on Location.

[13] https://www.facebook.com/help/325807937506242
[14] https://help.twitter.com/en/rules-and-policies/media-settings
[15] https://help.instagram.com/448523408565555
[16] https://www.linkedin.com/help/linkedin/answer/a1338882
[17] https://support.tiktok.com/en/account-and-privacy/account-privacy-settings
[18] https://m.facebook.com/help/www/1679637135584406
[19] https://help.x.com/en/resources/how-you-can-control-your-privacy
[20] https://help.instagram.com/627963287377328
[21] https://support.tiktok.com/en/account-and-privacy/account-privacy-settings/video-visibility

3. To turn off location services for all apps, toggle 'off" next to "Use Location" or "Location Services."
4. To turn off location services for specific apps, scroll down and select the app, then choose "Deny" or "Allow only while using the app" instead of "Allow all the time."

## 3.7 Remove Location Tags from Photos and Posts

Including location information in photos and posts can reveal more about you than you intend. You can manually add a location to a post if you want, but it's important to not allow this by default and to be judicious about including locations.

Remove location tags:

- Facebook[22]: As of 2011, Facebook strips geotag information from photos.
- X: The option to tag your location in Tweets on mobile is off by default, but you have the option to turn it on.
- Instagram[23]: You can set defaults as well as edit locations on existing posts.
- TikTok[24]: You can change this setting going forward, but as of June 2024, TikTok does not currently provide a feature to edit the geolocation tag after a video has been posted.

## 3.8 Family Members

Malicious actors can also target family members for cyber-attacks and social engineering. This becomes crucial when an election official's information is not publicly available, but family members post similar information, including addresses, locations, and times when they are not at home, such as during vacations.

They should adhere to the guidelines in this document, which include deleting old or unused social media accounts, limiting personal information shared, effectively using privacy settings, and exercising caution when accepting friend requests.

In addition, election officials should sit down with their family members to discuss the importance of privacy and the potential risks associated with a public digital footprint. Use the guidelines outlined in this document and the collective responsibility of enhancing their digital security and privacy.

[22] https://m.facebook.com/help/ipad-app/175921872462772
[23] https://help.instagram.com/841545179210359
[24] https://support.tiktok.com/en/account-and-privacy/account-privacy-settings/location-services-on-tiktok

CHAPTER

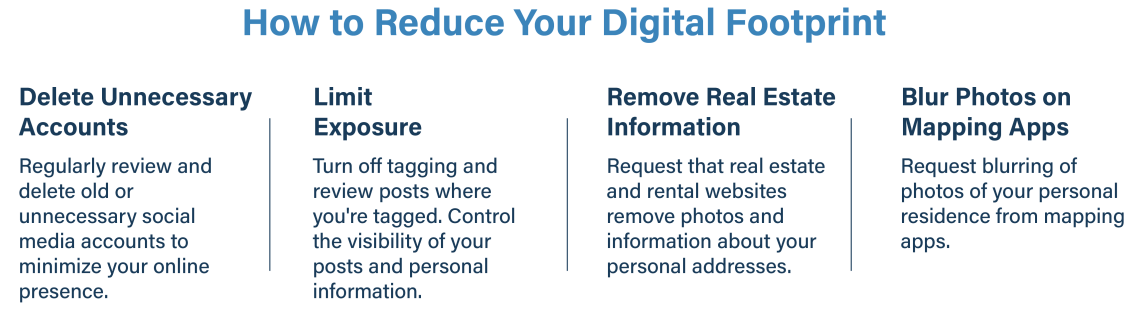
FOUR

# DIGITAL FOOTPRINT REDUCTION

Decreasing one's social media footprint and making accounts private can protect against identity theft, cyberstalking, and other malicious activities that can put personal information at risk. By implementing the recommendations outlined in this document, officials can mitigate risks, protect their personal information, and secure the privacy of themselves, their family members, their staff, and their organizations.

From understanding the importance of separating personal and office social media accounts to removing personal information from the public web and using privacy settings effectively, the following guidelines will empower elections officials to navigate the digital landscape securely and confidently.

In addition to the actions elsewhere in this document, consider reducing your social media footprint through each of the following actions.




## 4.1 Delete Social Media Accounts

Unless you're actively using a social media account and feel it benefits you, delete it. This is the most effective way to reduce your social media footprint and minimize your exposure to potential security risks. Accounts no longer in use leave data out there and each open account increases the risk of being part of a data breach.

Most platforms will allow you to export your data; make sure to back up any important data before proceeding. Also, some platforms may take a few days to weeks to completely remove your data, though they will typically immediately make it publicly unavailable.

Delete your account: Facebook[25] | X[26] | Instagram[27] | TikTok[28] | LinkedIn[29]

## 4.2 Limit Personal Information Online

Avoid posting sensitive information such as your home address, phone number, email address, and information about your family and their locations. Removing personal information from the public web can help prevent identity theft, cyberstalking, and other forms of online harassment. Here are some steps to remove personal information from the public web:

- **Query and Monitor Yourself**: Search for your name and see what information is available about you. The more common your name is, the more information you may have to include in the initial query to find information specific to yourself. Try different combinations such as with and without your middle name, your profession, or including cities or places of business with which you may be associated. Use multiple search engines such as Google and Bing, as they may return different results. After the initial pass, set up Google[30] (or other) alerts for your name and other personal information to monitor when it appears online to monitor for information about you continually.
- **Opt-Out of Data Brokers and People Finders**: Data brokers collect personal information from a variety of sources and sell it to third parties. Popular data brokers include Spokeo, Intelius, and BeenVerified. These services are required to provide a way for people to opt-out, though opting out of one data broker does not remove your information from all. Generally, just go to the site, search for your information, and follow the instructions to remove it. Alternatively, many third-party services, like DeleteMe, will continually scan sites and request removal of your personal information.

## 4.3 Removing Information from Real Estate Websites

Major real estate and rental websites post photos and information about addresses. Some allow you to request removal of your information. The removal process may take some time.

These sites often get their information from public records, so removing your information from these sites does not remove your information from public records. Even after removal, some details may remain in search engine caches and will disappear over time as those caches are updated.

Remove real estate data: Zillow[31] | Realtor.com[32] | Redfin[33] | Apartments.com[34] | Trulia[35]

[25] https://www.facebook.com/help/250563911970368
[26] https://help.x.com/en/managing-your-account/how-to-deactivate-x-account
[27] https://help.instagram.com/370452623149242
[28] https://support.tiktok.com/en/account-and-privacy/deleting-an-account/deleting-an-account
[29] https://www.linkedin.com/help/linkedin/answer/a1379064
[30] https://www.google.com/alerts
[31] https://zillow.zendesk.com/hc/en-us/articles/360040823574-How-do-I-delete-my-data
[32] https://www.realtor.com/advice/sell/how-do-i-get-a-real-estate-listing-removed-2/
[33] https://support.redfin.com/hc/en-us/articles/360013247432-Removing-Photos-on-a-Sold-Home
[34] https://propertyhelp.apartments.com/article/636-how-do-i-deactivate-my-listing
[35] https://support.trulia.com/hc/en-us/articles/216543357-How-do-I-remove-photos-of-my-home-from-Trulia

## 4.4 Blur Your Home Address on Google and Apple Maps

Here are the steps to blur your home address on Google Maps:

1. Open the Google Maps desktop app and make sure you're logged into your Google account.
2. Type your home address into the search field.
3. To see Street View's image of your home, select and hold your mouse pointer on the small yellow human icon at the lower right corner of the map.
4. Drag this icon onto the road in front of your home.
5. Once you're in Street View, use the arrow keys to rotate the view so you can see your home right in front of you.
6. Once you have your house in view, select "Report a problem" at the lower right corner of the screen.
7. You will see the image from Street View with a small red box at the center. You can rotate the image or zoom in and out to center the box on just your home or entire property.
8. Fill out the form by selecting "My home" in the "Request blurring" section.

Please note that once you complete this process, it can't be undone. Your home will be permanently blurred in Google Street View.

On Apple Maps, you can request to have a face, license plate, or house censored by emailing [MapsImageCollection@apple.com].