Managing Your Digital Footprint

A digital footprint is all the information that exists on the Internet because of online activity. This includes but is not limited to your social media posts, chats, texts, browsing history, emails, online purchases, and location data. Your digital footprint can:

- **Increase your risk of being scammed**. Scammers and fraudsters can use your digital footprint to target you, impersonate you, or steal your information.
- **Leave you open to surveillance, including by government agencies and abusive or controlling individuals.** This includes knowing where you are if your location is on or if you are “checking in” on social media.
- **Increase the likelihood of victimization.** Criminals use people’s digital footprint to target and lure them into forced or coerced work situations. Extremists and other bad actors can also use people’s digital footprint to target them for hate speech and hate crimes.
- **Negatively impact your immigration case.** Social media accounts, usernames/handles and other digital information must now be disclosed in connection with many common immigration applications, and electronic devices may be searched when an individual seeks to enter the US or is taken into Department of Homeland Security custody. Individuals’ online activity can be used to influence decisions about detention, deportation, adjustment of status, naturalization, asylum or other forms of immigration relief.

Managing your digital footprint is critical to your safety, security and reputation!

12 Tips for Managing Your Digital Footprint

1. **Protect your devices and accounts.** Make sure that all your devices have a strong password and ideally two-factor authentication. Two-factor authentication is when there are two authentication methods, like a password plus entering in a code you receive on your cell phone.

2. **Don't share private information.** Do not post your full name, address, phone number or other private information on the internet, including on social media.

   Don't tag your location on social media.

   Don't post photos that can identify where you are, live, work or attend school, such as house numbers, street signs, license plates, uniform logos, etc.

3. **Make your accounts private.** If you have social meeting accounts, make sure that they are private. Typically, you can do this by going to your account, going to Settings or Privacy, and making sure that 'private' is selected.

4. **Delete old accounts.** If you are no longer using an account, delete it. Similarly, disable cloud storage or accounts on any old devices that you may still have but rarely use.

5. **Turn off your location tracker.** To disable location tracking on a device, go to the device's settings, which is usually found under "Privacy," "Security," or "Location". From there, turn off Location Services to disable apps and services from knowing your location.

6. **Limit what you post.** Post a minimal amount of data online.

   Be careful about what you post as it may be misconstrued or place you at higher risk of being targeted. For example, posting a picture drinking alcohol, holding a gun, etc.

7. **Do not accept friend requests from people you don't know.** Make sure you only accept friend requests from people you know. Anyone can hide behind a profile including scammers, traffickers, and people trying to surveille you.

Delete friends from your accounts if you do not personally know them.

8. **Delete sensitive material and apps from phones and other devices**. If travelling internationally, Department of Homeland Security agents may search electronic devices at ports-of-entry upon re-entering the US. Delete all texts, photos, apps and other materials that may be misconstrued.

9. **Communicate securely.** Use communication apps that offer end-to-end encryption such as WhatsApp, Signal and Telegram.

   Note: Though more secure, even encrypted message platforms can contribute to your digital footprint through stored metadata like who you communicate with and when, as well as shared content such as videos, images and profile information. Be careful what you communicate.

10. **Be careful when navigating the web.** Don't click on suspicious links from senders you do not know or go to untrusted websites as these could open you to viruses and potential surveillance.

    Only provide necessary information and be very careful of websites or apps that ask for more personal information than is needed.

    Regularly clear your browser cookies and cache. You can typically do this by going to your Browser's Settings, then Privacy Settings, then find "clear browsing data" or a similar option.

11. **Use a temporary or disposable cell phone.** These phones are often prepaid and not tied to a contract, making them easier to use for anonymity and avoid tracking. However, if you use a temporary phone, be sure to make sure that people that need to reach you (caseworker, attorney, etc.) have your updated number. Sometimes, people choose to have two phones – a temporary phone for their online activity and a permanent phone for important and stable communication with key people.

12. **Use Camera Covers.** Use camera covers on phones and laptops to block the lens when not in use. This can prevent invasions of privacy.