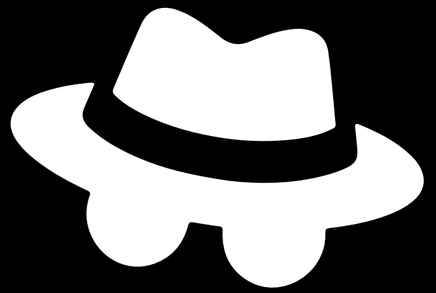
MPLP FIFTH FRIDAY TECH WEBINAR -

Digital Declutter: Cleaning Up Your Online Presence

SCOTT ELLIS

LAUREN MUNDY

DAN KEENER



MPLP

Michigan Poverty Law Program

INTRODUCTION

In today's interconnected world, your online presence is your professional and personal calling card. From old social media posts to outdated profiles and public information you didn't even know was out there, a messy digital footprint can cost you opportunities and compromise your privacy.

We will give a general overview of how to conduct a comprehensive audit of your current online footprint, actionable steps to lock down your social media settings and protect your personal data from prying eyes, and how to effectively remove unwanted content from the web.

STAYING SAFE ONLINE - DEFENDING AGAINST ONLINE DOXXING AND HARASSMENT - USE SIGNAL

- **Use encrypted messaging.** By using encrypted messaging communications where possible, you eliminate numerous sources of surveillance and tracking. Consider using Signal Private Messenger for encrypted voice, video, and text message communication. SMS (plain old “text messaging”) is not encrypted and can be read by your mobile provider, or any phone network provider or malicious government agency. Avoid SMS if possible! Email messages are typically unencrypted and can be read by your email provider and the recipient’s email provider. Many messaging apps other than Signal offer some level of encryption, but different platforms will leak different amounts of metadata (who is texting whom, at what time, and even address book data) to law enforcement.

- Apple iMessage offers encrypted messaging, but only to other iMessage users; it falls back to unencrypted messages to other people. WhatsApp messages are also encrypted, though its owner Meta has faced criticism for sharing data from WhatsApp with other Meta products (like Facebook and Instagram), as well as with law enforcement. As of 2025, Signal remains the best choice, but it only works when all of the people communicating use it.

SIGNAL'S CORE PRIVACY FEATURES

- End-to-End Encryption (E2EE): All messages, voice calls, and video calls are automatically secured using the open-source Signal Protocol. Only the sender and recipient can read or hear the content.
- Open Source: Signal's client and server code are publicly available for independent auditing, ensuring transparency.
- Minimal Data Collection: Signal is designed to collect and store the absolute minimum amount of metadata (e.g., it doesn't log IP addresses, or the content of your messages, calls, or groups).
- Usernames: Allows users to chat without sharing their phone number, adding a significant layer of privacy.
- Registration Lock (Signal PIN): A secure PIN that protects your account settings, profile, and contacts, and is required to register your number on a new device.
- Disappearing Messages: Automatically deletes messages for both the sender and recipient after a set, customizable time period (e.g., 30 seconds to one week).
- Screen Security: Can be enabled to prevent screenshots from being taken within the app on Android.
- Relay Calls: An optional setting to hide your IP address from the person you are calling by routing the call through a Signal server.
- Safety Numbers: A mechanism (QR code or numeric string) for users to verify that a contact's encryption key has not been compromised.
- Sealed Sender: A feature that conceals the sender's identity from Signal's servers.

SIGNAL'S MESSAGING & COMMUNICATION FEATURES

- Standard Messaging: Send text, voice messages, images, videos, GIFs, files, and contact cards.
- View Once Media: Allows sending photos or videos that can only be viewed one time by the recipient before they disappear.
- Group Chats: Supports large group chats (up to 1,000 members) with full E2EE and admin controls.
- Voice and Video Calls: Encrypted one-on-one and group voice/video calls (group calls support up to 40-50 participants).
- Stories: Allows sharing encrypted, disappearing images, text, and videos with selected contacts for 24 hours.
- Read Receipts and Typing Indicators: Can be individually enabled or disabled for more control over your privacy.
- Note to Self: A private chat for sending messages, photos, and files to yourself across linked devices.
- Image Blurring Tool: A simple editor that allows users to blur faces or sensitive information in photos before sending them.
- Cross-Platform Support: Available for Android, iOS, Windows, macOS, and Linux.

STAYING SAFE ONLINE - DEFENDING AGAINST ONLINE DOXXING AND HARASSMENT - PRIVATE BROWSING

- **Don’t sign into your web browser.** Signing into your browser, especially if it is operated by a surveillance economy company, as Chrome is operated by Google, allows the browser vendor to easily track what you do and where you go online. Sign in only when you specifically need to do so, and sign out afterwards. Consider also using a web browser that is not maintained by a surveillance-economy company. Firefox, Brave, and Tor Browser are all web browsers that are more respectful of your data and your privacy than other major browsers. It’s perfectly fine to have multiple web browsers; try using different ones.
- **Make use of your browser’s “private browsing” or “incognito” mode.** Using this setting where possible won’t protect you from all tracking by services you use within the session (or from tracking by your network provider), but it will avoid leaving traces on your local machine. Using private browsing mode also means that if you do identify yourself to a service during that session (e.g., by logging in to a web site), that identification is less likely to be linked to your activities in other sessions.
- Use document colaboration that doesn’t track you like Framapad or Cryptpad. Neither of these services will build profiles of you for targeting purposes, or associate your identity with the contents of your documents.
- Delete cookies and browsing history. By deleting all of your cookies as well as your browsing history, you can reset the memory of the browsers that track you across the web.

https://www.aclu.org/news/free-speech/some-steps-to-defend-against-online-doxxing-and-harassment

SELECT A TRULY PRIVATE VPN

Choosing a Virtual Private Network (VPN) for privacy requires careful consideration of several key factors, as the VPN provider becomes your new "Internet Service Provider" and can potentially see your online activity. The main privacy considerations are:

🔒 Logging Policy

- The most critical factor is the VPN's logging policy. A trustworthy, privacy-focused VPN should have a strict "No-Logs" policy.
- Activity Logs (Usage Logs): This is the most sensitive data, including your browsing history, connection times, data transferred, and the websites you visit. A strict no-logs policy means the VPN does not record this information, making it impossible for them to tie online activity back to you.
- Connection Logs (Metadata Logs): These are less invasive and sometimes kept to maintain service quality. They might include timestamps of connections, server location used, and bandwidth consumption. Ideally, a privacy VPN keeps minimal to zero connection logs, and any logs kept should be non-identifying and temporary.
- Independent Audits: Look for VPNs that have had their no-logs claims and security infrastructure verified by a reputable, independent third-party auditing firm. This provides an objective confirmation that the policy is being followed.

SELECT A TRULY PRIVATE VPN - CONT.

🛡️ Technical Security Features

The technologies used by the VPN directly impact your privacy and security.

- Encryption Standard: The gold standard is AES-256 encryption, which is used by governments and financial institutions. Avoid VPNs using weaker or outdated methods.
- Kill Switch: This is an essential feature. A kill switch automatically cuts your internet connection if the VPN connection unexpectedly drops, preventing your real IP address or unencrypted data from leaking to your ISP or others.
- RAM-Only Servers: Some premium VPNs use servers that run entirely on RAM (Random Access Memory), which means data is never written to a hard drive and is wiped clean every time the server is restarted. This ensures no data remains to be seized or compromised.
- VPN Protocols: Look for modern, secure protocols like OpenVPN and WireGuard.

💰 Business Model and Payment

How the company makes money and accepts payment can offer clues about its commitment to privacy.

- Paid vs. Free: Be extremely cautious of free VPNs. If you're not paying for the service, the business model may involve selling user data or serving targeted ads, directly compromising your privacy.

SELECT A TRULY PRIVATE VPN - CONT.

Here are some of the most prominent VPNs with independently audited No-Logs policies, including information on their most recent public audits:

VPN Provider	Jurisdiction	Most Recent Audit (Type/Firm)	Key Takeaway
NordVPN	Panama	Late 2024 (No-Logs Assurance by Deloitte)	Successfully passed its fifth No-Logs assurance assessment, verifying that no activity logs are kept.
Proton VPN	Switzerland	August 2025 (No-Logs Audit by Securitum)	Passed its fourth consecutive annual No-Logs audit, confirming no collection of activity or metadata logs. Their apps are also open-source and audited.
ExpressVPN	British Virgin Islands	Early 2025 (TrustedServer & No-Logs Assessment by KPMG)	The audit verified their TrustedServer technology (RAM-only servers) is engineered to prevent the collection of activity and connection logs.
Surfshark	Netherlands	Mid-2025 (No-Logs Assurance by Deloitte)	The independent verification confirmed their adherence to their no-logging claims and privacy policy.
Private Internet Access (PIA)	United States	Ongoing (Open-Source Apps/Infrastructure)	While based in the US, PIA's No-Logs claim has been proven twice in court by US authorities being unable to produce logs when subpoenaed, in addition to being open-source.
Mullvad	Sweden	Multiple Audits (Infrastructure/Security by Assure, Cure53)	Known for an extremely strong privacy stance (no email sign-up, cash payments). They conduct regular, public infrastructure and security audits.

EMAIL PRIVACY - PROTON MAIL

Proton Mail is widely regarded as one of the most privacy-focused email services available, and it is built around core principles that differentiate it from major providers like Google (Gmail) or Microsoft (Outlook).

Here is a breakdown of the key factors that make Proton Mail truly privacy-focused:

1. 🛡️ Foundational Encryption & Zero-Access
   - End-to-End Encryption (E2EE): When you send an email to another Proton Mail user, the message is encrypted on your device and only decrypted on their device. Neither your ISP, nor Proton, nor any third party can read the content during transit or storage.
   - Zero-Access Encryption: Even if an email arrives unencrypted (e.g., from a standard Gmail account), Proton Mail immediately encrypts the content on its servers using your public key. Because Proton does not have access to your private decryption key (which is protected by your user password), they physically cannot decrypt or read the contents of your stored messages.
2. 🔍 Open-Source & Audited
   - Proton commits to transparency, allowing its security claims to be verified by the public.
   - Open Source: All of Proton's applications and cryptographic libraries are open source. This means that independent security researchers can inspect the code to verify that it works as promised and doesn't contain hidden backdoors or logging mechanisms.
   - Independent Audits: Proton regularly undergoes independent security audits by third-party firms to vet its security architecture.
3. 📝 Business Model
   - Proton Mail is a paid service (with a generous free tier) supported entirely by its user community, not advertisers.
   - The company's revenue comes from subscriptions, ensuring that its business interest is aligned with protecting user privacy rather than exploiting user data for targeted advertising.

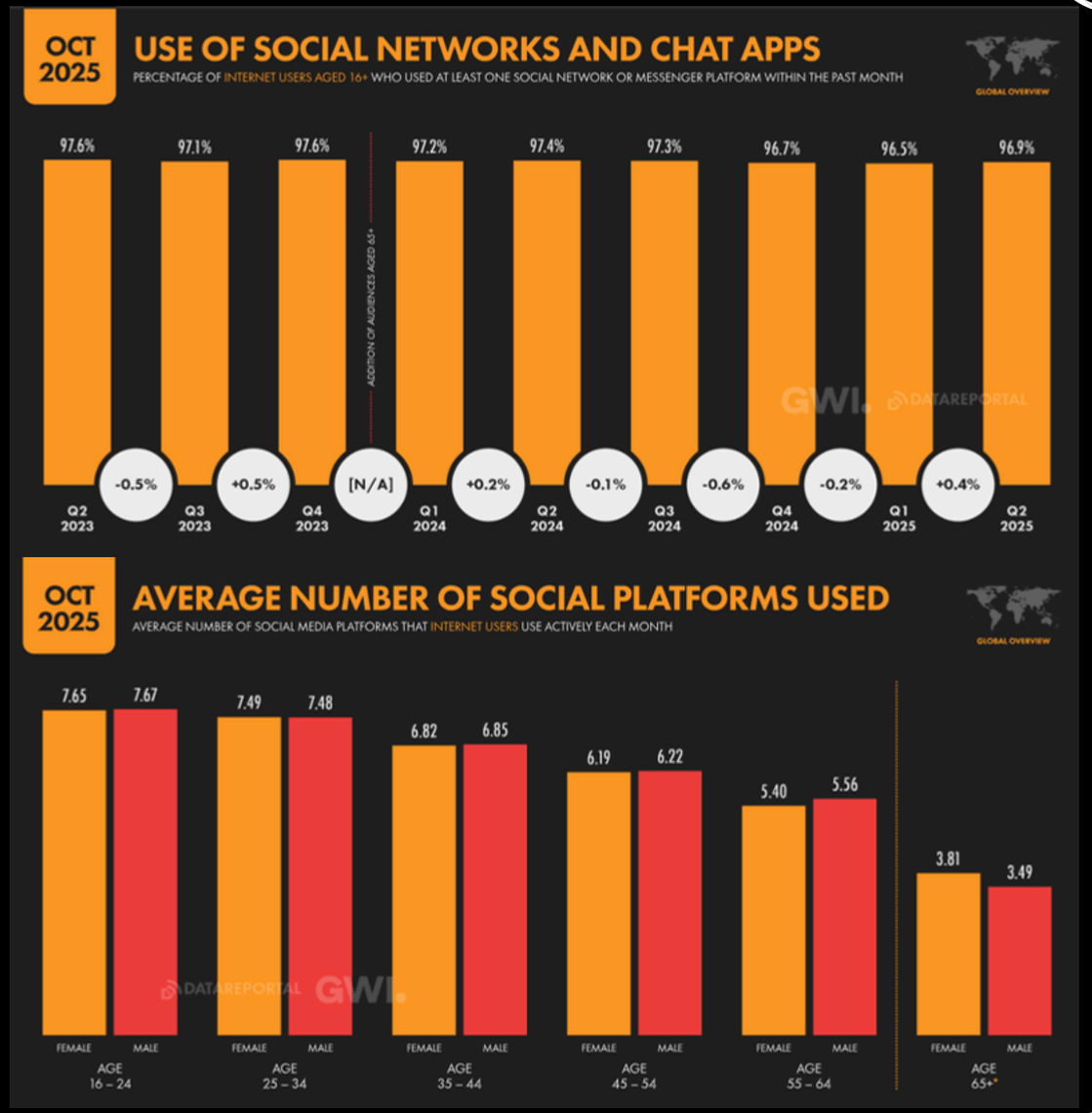
DIGITAL SECURITY AND SOCIAL MEDIA

According to a 2024 Pew Research survey, 79% of internet users are concerned about how companies use their personal data, yet 40% of users do not regularly check their privacy settings.

An unmanaged social media footprint can have multiple consequences including identity theft, social engineering attacks, data breaches, and even real life safely concerns.

One critical difference with a digital footprint is its permanence. Digital traces can remain accessible indefinitely. Deleted posts might be archived, re-shared, or indexed by search engines, making complete erasure a difficult and complicated task.

Managing your social media data is not about disconnecting from the digital world, but engaging with it intentionally and securely.



SOCIAL MEDIA SECURITY

- Facebook
  - You can use the Privacy Checkup tool to review security and privacy settings. Limit posts and people who can see your profile information to only "Friends". Turn on timeline review to approve or dismiss content you are tagged in before they appear on your profile.
- Instagram
  - Set your account to Private. A private account requires you to approve followers, and only people you approve can comment on your posts.
- Twitter (X)
  - Set your posts to Protected. When tweets are protected people cannot retweet you, and they can only view your tweets if you approve them to follow you. Protected posts will only be visible and searchable by you and your followers, and will not appear in search engines.
- TikTok
  - Set your account to "Private" so only approved people can follow you and view your videos. Turn off "Allow others to find me" to help stop people you don't know from seeing your profile.
- WhatsApp
  - Change "Last seen", "Profile photo and info about you", and other settings to "My Contacts" only. Turn off "Live location" sharing.
- LinkedIn
  - Avoid oversharing specific details that could give information that enables impersonation. Manage your Sign in & security settings and control Visibility (who can see your profile and network)

ADDITIONAL SOCIAL MEDIA SECURITY TIPS!

For personal use -

- If you need (or simply just want) to keep your social media accounts public, consider using a fake name/pseudonym.
- Never publicly share your personal phone number or address on social media.
    - Be mindful of specific location information you share on posts. Photos with the outside of your residence could be used to find your address even if you never specifically give it.
- If you have social media accounts that you no longer use, delete them.
    - Unmanaged and unmonitored accounts are prime targets for identity theft.

For business accounts -

- Make sure the account security complies with your organization’s security policies.
- Give administrative rights only to select staff whose roles require it. Review and update access rights regularly.
    - If more than one person is responsible for an account, use a password manager where you can securely share login information.
- Consider implementing a content approval process before publication.
- Avoid using non-organization owned emails and phone numbers for work-related social media accounts.

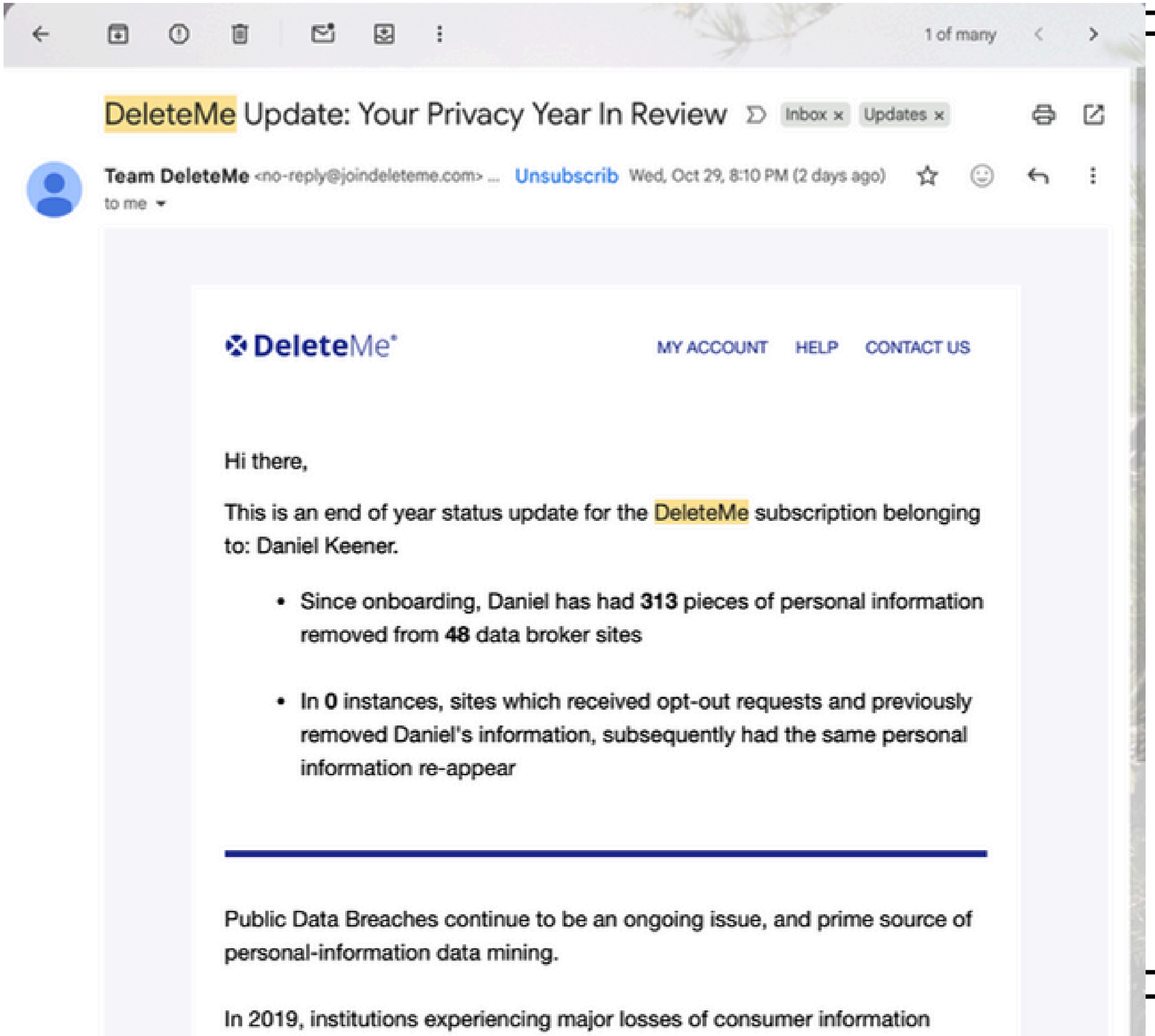
DELETE ME

- Submit your personal information for removal from search engines and data broker sites.
- DeleteMe experts find and remove your personal information.
  - They remove private information from 850+ different Data Brokers
    - Data brokers are companies that gather large amounts of personally identifiable information (PII) from a wide range of sources. Their business is to collect, analyze, and sell or license your personal data to anyone willing to pay for it.
- You would receive a detailed DeleteMe report in as little as 7 days.
- DeleteMe continues to remove your personal info regularly, all year long.
- DeleteMe cannot delete Google search results themselves without first removing the source information that the search result is pulling the information from, the data broker websites.
  - Google has their own Search Result delete tool at https://myactivity.google.com/results-about-you

DELETE ME OVERVIEW

- Be sure to provide as much detail as possible (i.e. past addresses, aliases, misspellings of your name, etc.)
- There is a section that says 'Privacy tools' that has a lot of cool features that people can use like email masking, phone masking, and searching yourself and removing that information from the web.
- The first report takes about a month to complete. Once you receive your report make sure you update any pieces to your data sheet so that the next report is more accurate as well.

EXAMPLE EMAIL



1 of many

DeleteMe Update: Your Privacy Year In Review

Inbox × Updates ×

Team DeleteMe <no-reply@joindeleteme.com> ... Unsubscrib Wed, Oct 29, 8:10 PM (2 days ago)

to me

DeleteMe®

MY ACCOUNT HELP CONTACT US

Hi there,

This is an end of year status update for the DeleteMe subscription belonging to: Daniel Keener.

- Since onboarding, Daniel has had **313** pieces of personal information removed from **48** data broker sites
- In **0** instances, sites which received opt-out requests and previously removed Daniel's information, subsequently had the same personal information re-appear

---

Public Data Breaches continue to be an ongoing issue, and prime source of personal-information data mining.

In 2019, institutions experiencing major losses of consumer information

DeleteMe

Dashboard
Reports
Privacy Tools
Data Sheet
Account
Family & Referrals

Sarah Robbins
Privacy Advisor
Make a Request

Privacy Dashboard

Daniel Keener

Your last report

Done on Aug 05

View Report

Your subscription

Update

Since Nov 18, 2024

Standard Protection
Renewal on Nov 18, 2025

1 Person(s)

Add a family member

Is this your phone?

See all

Found on 02/04/2025 at Neighbor Report

+1 614-284-2927

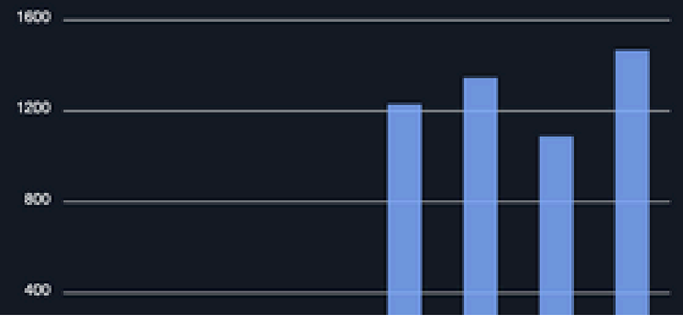
Yes, my mobile
Yes, my landline
No

94
TOTAL DATA BROKERS

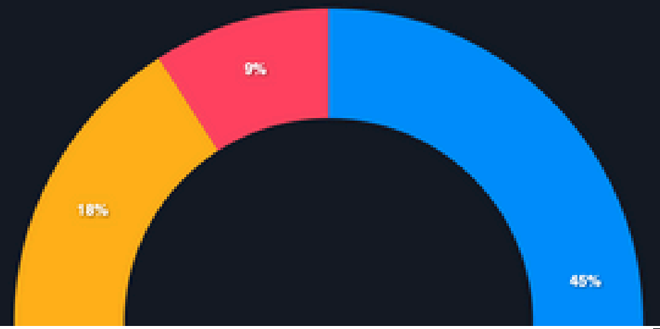
5,133
LISTINGS REVIEWED

46
DATA BROKERS WITH YOUR INFO

Listings Reviewed



Your exposed data



Report Findings

2025

411COM

APPROX REMOVAL TIME

14 Days

PERSONAL INFO EXPOSED

Name	Photos
Age	Email
Address	Past Address
Phone	Occupation
Relatives	Marital Status
Spouse Name	Propty. Value
Social Media	Court Records

REMOVAL IN PROGRESS

AnyWho

APPROX REMOVAL TIME

3-5 Days

PERSONAL INFO EXPOSED

Name	Photos
Age	Email
Address	Past Address
Phone	Occupation
Relatives	Marital Status
Spouse Name	Propty. Value
Social Media	Court Records

REMOVAL IN PROGRESS

FreePeopleDirectory

APPROX REMOVAL TIME

3-5 Days

PERSONAL INFO EXPOSED

Name	Photos
Age	Email
Address	Past Address
Phone	Occupation
Relatives	Marital Status
Spouse Name	Propty. Value
Social Media	Court Records

REMOVAL IN PROGRESS

Privacy Tools

Daniel Keener

Email Masking

Stop spam by keeping your email private

See More →

Search Yourself

Find and remove your personal information from the web

See More →

Phone Masking

Keep your number private and end the 8AM telemarketing

See More →

Card Masking

Pay anywhere without revealing your credit card

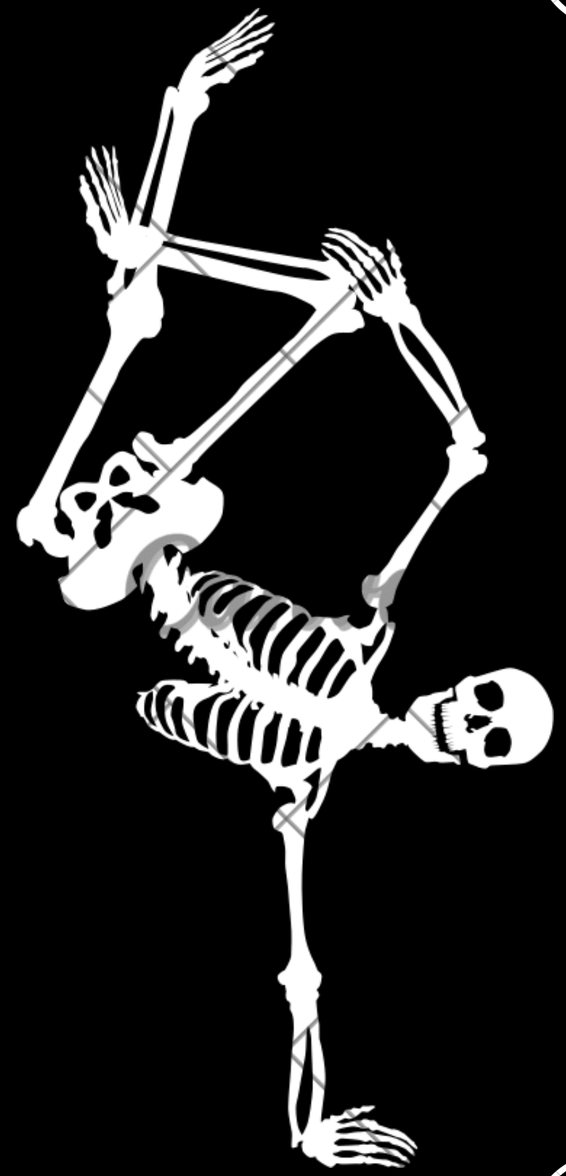
Coming Soon

THANKS

Scott Ellis, scoellis@lsscm.org
MAP IT Systems Administrator

Lauren Mundy, lmundy@lsscm.org
MAP Operations Manager

Dan Keener
MIRC Systems & Admin Supervisor



RESOURCE PAGE

- National Cyber Security Centre Social Media guidance
- How To Protect Your Digital Footprint
- How To Manage Your Digital Footprint: 20 Tips for Students
- 2026 (Oct 2025) Global Digital Overview Report
- https://www.aclu.org/news/free-speech/some-steps-to-defend-against-online-doxxing-and-harassment
- Google Results About You page
- DeleteMe
- https://github.com/anitwek/alternatives-to-us