IDENTITY THEFT TODAY

Managing Your Digital Footprint and Reducing Online Exposure

July 15, 2026
12pm - 1pm EST

LEGAL RESOURCES

SESSION NOTES

Below is a summary of the topics and audience questions from the July 15, 2026 session of **Identity Theft Today**, featuring guest speaker Ian Flanagan of Iris® Powered by Generali.

SESSION TOPICS

Digital Footprints | Data Breaches | Data Brokers | Social Media | App Tracking
Public Records | Social Logins | Old Accounts | Getting Started

Click Here to Access Recorded Session ⟶

UNDERSTANDING YOUR FOOTPRINT

- A digital footprint is the sum of small, everyday online actions — signing up for accounts, posting to social media, shopping, and other public activity.
- Individually these feel harmless, but combined they create a spectrum of risk: targeted advertising on the low end, escalating to fraud, scams, stalking, and identity theft on the high end.
- The goal is not to avoid the internet, but to know what is out there, stay aware, and build habits that reduce the exposure you are not comfortable with.

BREACHES AND BROKERS

- Data breaches expose personally identifiable information — Social Security, bank, and credit card numbers, and passwords — when organizations are hacked. Users have little control at the source but can monitor with an identity monitoring service or free tools like Have I Been Pwned.
- Watch especially for plain-text passwords in a breach: reset those accounts immediately and turn on multifactor authentication to add a second layer of security.
- Data broker and people-search sites aggregate and sell your information. Search your own name periodically (with an address or phone number), submit opt-out and removal requests, and expect to re-check, since sites often repost.
- Paid removal services — and, increasingly, AI tools — can automate opt-outs and monitor for reappearance. California's new deletion law and its DROP platform give residents a single place to opt out.

EVERYDAY TRACKING CHOICES

- Social media: set profiles to private, review who can see your content, and audit your friends and connections list — shared connections lend false legitimacy to stranger requests. Consider posting trips after the fact and turning off automatic location tagging.

- Apps and devices: many apps request more data than they need. Review permissions and toggle off anything beyond an app's scope, and disable or reset your phone's advertising identifier.
- Browsers and websites: cookies and trackers build a cross-site profile of you. Use built-in tracking protection, reputable extensions such as the EFF's Privacy Badger, and clear cookies and history periodically.

RECORDS AND ACCOUNTS

- Public records (home ownership, court filings, voter registration) are legally searchable and easily scraped. You cannot remove them, so focus on monitoring for changes rather than the source.
- Third-party social logins (Google, Apple, Facebook) are convenient but concentrate risk in a few keystone accounts — periodically review and revoke apps connected to them.
- Old, forgotten accounts fuel credential-stuffing attacks. Clean them up, search your inbox for old "welcome" emails, and let a password manager flag reused passwords.
- Connected devices and smart TVs (through automatic content recognition) collect usage data. Review privacy settings, and re-check them after software updates, which can quietly reset your choices.

WHERE TO START

- Start small and prioritize the highest-impact areas: secure your key accounts, check whether you have appeared in breaches, and tighten the privacy settings on the tools you use every day.
- Awareness and continual monitoring are key — automating removals and alerts turns an initial burst of effort into low-maintenance upkeep.

KEY ONLINE RESOURCES

- **Have I Been Pwned** — Free tool to check whether your email addresses or passwords have appeared in known data breaches. *haveibeenpwned.com*
- **Electronic Frontier Foundation** — Nonprofit offering practical privacy guidance and the free Privacy Badger browser extension, which blocks trackers. *eff.org* | *privacybadger.org*
- **Federal Trade Commission** — Consumer resources on data security and privacy, plus step-by-step identity theft recovery. *consumer.ftc.gov* | *IdentityTheft.gov*
- **Wikipedia: Digital Footprint** — A plain-language overview of the topics covered in this session, useful for review. *en.wikipedia.org/wiki/Digital_footprint*
- **California DROP** — For California residents, a single request that directs registered data brokers to delete your personal information. *privacy.ca.gov/drop*

Q&A HIGHLIGHTS

Q1. With so little regulation, how successful are opt-out requests to data broker sites?
A: Most sites are responsive because they are still obligated to honor removal and opt-out requests — but the larger ones often wait out the opt-out period and then repost, so staying on top of them (or paying a service to) is essential.

Q2. What is the difference between opt-out services and the Do Not Call list?
A: The Do Not Call list is passive — marketers are expected to reference it before cold-calling. A paid opt-out service is active: it continually scans for new brokers, submits removal requests on your behalf, and re-submits when your information reappears, more like an ongoing subscription.

Q3. What is a passkey?
A: A passkey is a digital identifier tied to your account and your specific device, used in place of a password. Because there is no password to steal, a passkey exposed in a breach is largely useless to an attacker who does not have your original device.

Q4. Is freezing your credit a good idea?
A: Yes — a freeze adds friction against anyone trying to open an account or pull your credit file in your name, and it gives you more control and awareness. You can temporarily lift it for legitimate needs, such as applying for a mortgage.

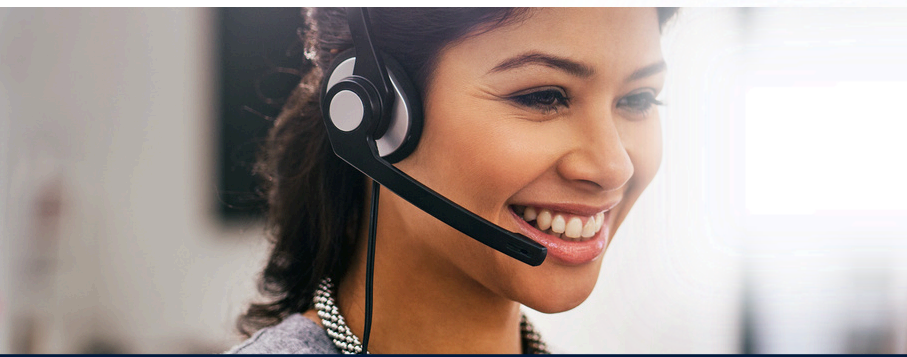
Q5. Can someone really steal my home's deed?
A: Home title fraud does exist, though titling companies make it difficult. Look up where your county keeps your title record, consider a title-monitoring service, and check whether your county offers a free change-notification service.

ABOUT THE SPEAKER:

IAN FLANAGAN | IRIS® POWERED BY GENERALI

Ian has spent roughly six years at Iris® Powered by Generali, a provider of identity monitoring solutions that help users detect data exposure, protect their personal information, and recover in the event of identity theft or fraud. IRIS is Legal Resources' service and technology partner for its identity theft protection benefit. Attendees with questions may contact Legal Resources for more information or a referral.

DISCLAIMER: This summary highlights key webinar points and questions. For comprehensive details, view the full seminar at **LRSeminars.com.**



Contact Us

Our Member Services team is available for assistance.

Phone: 800.728.5768
Email: info@legalresources.com

www.legalresources.com