# IDENTITY THEFT TODAY

## Understanding and Using Private Virtual Networks

July 16, 2025
12pm - 1pm

LEGAL RESOURCES

### SESSION NOTES

Below is a summary of the topics and items discussed on the July 16, 2025, session of ***Identity Theft Today: Understanding and Using Private Virtual Networks.***



### SESSION TOPICS

VPN Fundamentals | Online Privacy Protection | Public Wi-Fi Security | VPN Provider Selection | Common Misconceptions

**Click Here to Access Recorded Session** ⟶

## ONLINE PROTECTION

Your digital activities create valuable data trails that multiple entities collect and use. When you conduct online banking, shopping, or telehealth visits, you're transferring data between your device and web services through your Internet Service Provider (ISP). This information is captured and used by:

- **ISPs and websites** - Build online profiles to sell to advertisers and curate targeted content
- **Government agencies** - Leverage data for surveillance purposes
- **Cybercriminals** - Use stolen PII to conduct identity fraud and financial crimes

VPNs provide one layer of protection in your overall cybersecurity strategy, though they're not a complete solution for all online threats.

## VPN FUNDAMENTALS

**What is a VPN?** A Virtual Private Network creates a secure, encrypted connection between your device and the internet. Originally developed for businesses to allow remote employees safe network access, VPNs have become popular among consumers as cyber threats have increased.

**How VPNs Work:** VPNs function as an intermediary between your device and the internet by:

- **Masking your IP address** - Websites see the VPN server's IP instead of your actual location
- **Encrypting your data** - All information is scrambled, making it unreadable if intercepted

Without a VPN, your ISP sees every website you visit, your exact location, and timestamps of all activities. This unencrypted data flows to websites and can be intercepted by bad actors.

### Privacy Benefits

**Data Protection:** In the United States, ISPs can legally capture and sell your browsing data to advertising companies and data brokers. This information is extremely valuable because it helps companies understand your behavior and target you with products and ads.

**Geographic Access:** VPNs allow you to access content from different geographic locations by connecting through servers worldwide. For example, streaming services like Netflix offer different content libraries in different countries.

**Censorship Circumvention:** In countries with authoritarian regimes that restrict internet access, VPNs enable users to access content beyond government-imposed limitations.

## Public Wi-Fi

**Security Risks:** Public Wi-Fi networks, especially those without passwords, present significant security vulnerabilities:

- **Unencrypted data** - Your information travels in readable format
- **Man-in-the-middle attacks** - Bad actors can intercept data between your device and the network
- **Rogue access points** - Criminals create fake hotspots specifically to capture user data

**VPN Protection:** When using a VPN on public Wi-Fi, your data remains encrypted even if intercepted. While attackers might still capture your data flow, they'll only see scrambled, unusable information.

## Provider Selection

**Essential Features:**

- **No-logs policy** - Provider doesn't track or store your activities
- **Strong reputation** - Established company with positive consumer reviews and no breach history
- **Robust encryption** - Advanced security protocols and regular software updates
- **Multiple server locations** - Global network for geographic flexibility

**Additional Considerations:**

- Customer support availability
- Transparent pricing with trial periods
- Compatible apps for all your devices
- Additional features like ad blocking or malware protection

**Red Flags:**

- Completely free services (often monetize your data)
- Vague privacy policies
- History of security breaches
- Companies based in high-surveillance countries
- Forced browser redirects or excessive advertising

## Common Misconceptions

- **"All VPNs are trustworthy"** - Many free VPNs actually sell user data, defeating the privacy purpose. Research providers carefully.
- **"VPNs provide complete anonymity"** - Websites can still identify you through login credentials and track your behavior within their platforms.
- **"VPNs prevent all cyber threats"** - VPNs protect data transmission but don't prevent malware downloads, phishing attacks, or website breaches.
- **"VPNs make you invisible to employers/ISPs"** - Your ISP and network administrators can detect VPN usage, though they can't see your specific activities.

## Implementation Options

**Consumer VPN Apps (Easy):** Download from reputable providers, click connect, optionally select server location. Most user-friendly approach costing $5-12 monthly.

**Enterprise VPN (Medium):** IT departments configure VPN directly on devices for business use. Requires technical assistance.

**Router Configuration (Hard):** Install VPN directly on router to protect all connected devices including smart TVs and gaming consoles. Requires technical expertise.

## Q&A Highlights

**1. How do I keep my phone safe for online purchases since it doesn't have the same security as my computer?**

**Answer:** VPNs work identically across all devices - your data remains encrypted whether you're using a phone or laptop. However, VPNs are just one security tool. For comprehensive phone protection: keep your mobile OS updated with latest security patches, audit app permissions carefully (revoke unnecessary access to files and photos), enable biometric authentication for banking apps (Face ID/fingerprint), and use multi-factor authentication. Even with a VPN, you can still click malicious links or become a victim of website breaches.

### Coming Up Next Month

**Trending Threats**

August 20, 2025
12pm - 1pm

*Register at www.LRseminars.com*

**2. Are web browsers like Safari really transferring information that cannot be seen by others?**
**Answer:** Browsers promoting "secure browsing" like Safari or DuckDuckGo provide some additional privacy features like ad blocking or limited built-in VPN functionality, but they're not equivalent to standalone VPN applications. Your ISP still receives significant browsing information through DNS lookups - when you visit amazon.com, your ISP must translate that to an IP address, revealing your destination. Many browsers' security features only protect traffic within that specific browser, while other apps and browsers remain unprotected.

**3. Do you recommend any specific VPN providers?**
**Answer:** Rather than endorsing specific brands, we recommend consulting reputable comparison sites like TechRadar and Security.org that provide detailed feature-by-feature analysis of top providers. Look for services that have been independently audited, maintain transparent no-logs policies, and offer open-source software that anyone can inspect. Some providers run servers entirely in memory, ensuring data disappears upon restart. ProtonVPN, NordVPN, and Private Internet Access are examples of providers that have undergone security audits and been reviewed extensively, though you should research current comparisons before choosing.

**4. What are some free VPN providers to avoid?**
**Answer:** Many reputable VPN providers offer limited free plans (slower speeds, fewer server locations) to let users test their service before purchasing. However, completely free VPN services often monetize by selling user data or displaying excessive advertising. Instead of seeking free options, consider that most quality VPN services cost only $5-10 monthly, or $10-12 annually. Before selecting any provider, verify their no-logs policy, check for independent security audits, and ensure they're not based in high-surveillance countries.

**5. Does Legal Resources' identity theft protection include VPN services?**
**Answer:** Yes, our Platinum plan for identity theft protection includes VPN services as part of the comprehensive protection package. Legal Resources offers three tiers: Basic, Gold, and Platinum. The Platinum plan is our top tier and includes VPN functionality along with other identity protection features. Check with your employer to see which plan they offer as part of your benefits package.

## About Our Speakers:

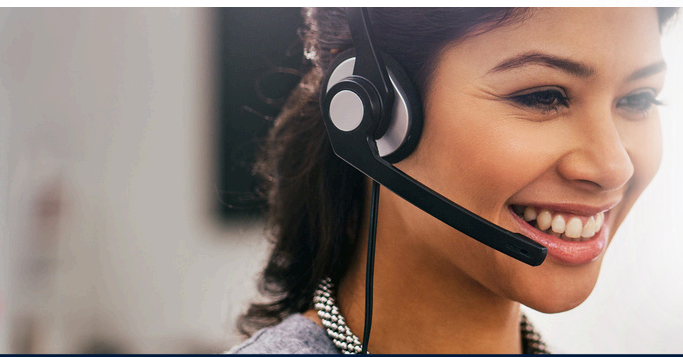
**YUWEI LI | PRODUCT MANAGER, IRIS IDENTITY PROTECTION**

Yuwei manages a suite of cybersecurity tools for end users at Iris Identity Protection, powered by Generali. She graduated from Notre Dame and earned her MBA from the University of Michigan.

**AMEER MASHKOUR | PRINCIPAL SECURITY ARCHITECT, IRIS IDENTITY PROTECTION**

Ameer brings over 20 years of experience in IT and cybersecurity, including extensive enterprise VPN implementations. He serves as Principal Security Architect at Iris Identity Protection.

**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