



THE LEGAL INVESTIGATOR

Journal of the
NATIONAL ASSOCIATION OF
LEGAL INVESTIGATORS

YOUR PRIVACY SOFTWARE IS
WATCHING YOU
WARNING: THE SUBJECT OF YOUR
INVESTIGATION MAY BE ALERTED
THAT YOU ARE RESEARCHING THEM
– BY LAEL HENTERLY, CLI - PG. 14

FALL 2025

AN OFFICIAL PUBLICATION OF THE NATIONAL ASSOCIATION OF LEGAL INVESTIGATORS, INC.



Your Privacy Software Is Watching You

Warning: The subject of your investigation may be alerted that you are researching them

By Lael Henterly, CLI

Within 45 minutes of David Jude entering a Social Security number into Delvepoint—a database for professional investigators—his cover was blown. The Lexington, Kentucky legal investigator was conducting an asset search in a divorce case when his client received a text: the estranged wife knew she was being investigated and named Jude's firm.

Days later, the woman called his office threatening lawsuits, claiming police were arriving with paperwork. They never came, of course, but the breach left Jude questioning the tools his profession depends on.

Pattern, Not Glitch

Washington investigator Wolfgang Grasst triggered a Credit Karma alert while searching Delvepoint through Microsoft Edge. His client questioned his methods; his reputation took a hit.

"Having a subject learn about an investigation compromises everything," Grasst says. "Your agency loses credibility."

When Jude contacted Delvepoint, their response proved useless—denying data sales while missing the point. "There's safety issues here," Jude told them. "Your product just exposed me." The representative didn't grasp the stakes.

The Common Thread

Jude's query to the National Association of Legal Investigators revealed a systemic problem. Responses varied—some investigators receive alerts so frequently they ignore them—but one name emerged repeatedly: LifeLock.

"Some say 100% LifeLock gets notified," Jude says. "Others say the opposite."

The pattern suggests identity monitoring services, browser extensions, and antivirus software form an inadvertent surveillance network, alerting subjects when their information is accessed—turning privacy protection into its own form of exposure.

The Network Emerges

Multiple legal investigators contacted David Jude after his exposure, confirming a pattern: identity monitoring services track Social Security numbers through unconventional methods. What appeared accidental looked increasingly deliberate.

LifeLock advertises data broker search alerts, promising to warn users when their personal information "appears online." Its new Privacy Monitor Assistant claims to scan hundreds of people-search sites including BeenVerified, Intelius, TruthFinder, and Radaris—platforms some investigators use. Conspicuously absent: professional databases like TLO, IRBSearch, and Delvepoint.

Attempts to reach LifeLock's product team dead-ended. Phone numbers disconnected. Emails vanished. The contacts from their press release had disappeared.

The Information Advantage

LifeLock's parent company faces an existential challenge. Credit bureaus launched competing identity services, forcing LifeLock to rely on rivals for alert data. After Symantec sold its enterprise business to Broadcom in 2019, it renamed itself NortonLifeLock and pivoted to consumers. The 2022 Avast merger created Gen Digital—consolidating cybersecurity brands under one surveillance umbrella.

Gen Digital's acquisitions reveal its strategy: Avast and Avira track browsing; MoneyLion's shopping extensions monitor purchases. Each product feeds the ecosystem. Court filings in federal consumer and patent matters expose how this apparatus provides "granular access" to customer web activity.

The Guardians Who Watch You

Identity monitoring services and antivirus products claim to protect privacy while tracking millions of users' web activity. Court filings reveal how Gen Digital built this surveillance apparatus.

In 2020, journalists exposed Avast collecting "full clickstream data" on millions of users. Its subsidiary Jumpshot sold this data to hedge funds, promising clients they could "jump the garden wall" to view competitor sites. Mozilla, Apple, and Opera banned Avast's extension. The FTC fined the company \$16.5 million in 2024.

Avast Online Security & Privacy remains available for Edge and Chrome, boasting 400 million users. Microsoft's continued hosting signals its stance on extensions that collect personal data.

Jumpshot shuttered, but litigation reveals the collection continued at Avast. Court-submitted packet captures show Avast's extension using server-to-server tracking—invisible data transfers between companies' backends that bypass browser privacy tools—to hoover up user's queries and clicks. Configuration choices, like setting cookie domains to "avast.com," ensured tracking identifiers traveled automatically to collection servers.

Setting cookie domains to "avast.com" ensured tracking identifiers reached collection servers automatically. One line of code—credentials: "omit"—would have prevented cookie transmission. Avast implemented it only after lawsuits began.

The data isn't sold; it circulates through Gen Digital's ecosystem. What enters through Avast exits through LifeLock as identity alerts—a digital ouroboros consuming its tail.

Beyond Browser Extensions

"It's tracked to Social Security numbers," Jude says—a capability investigators themselves lack. He adjusted his protocol after the breach, avoiding SSN searches when other identifiers suffice. Based on technical documentation from the patent lawsuits, it appears this is how it may have happened in Jude's case:

1. The investigator searches for an SSN on Delvepoint
2. If Avast's extension is installed, it captures the URL containing the SSN
3. The data flows to Avast servers with identifying cookies attached
4. Through server-to-server connections, the SSN sighting propagates to monitoring databases
5. LifeLock, checking those same databases, fires an alert to the subject

Yet Jan Barefoot, a legal investigator in Charlotte, N.C., triggered a LifeLock alert using only name and city. While vetting a subject using TLO, she entered no Social Security number, used Chrome without extensions—and yet her search was still exposed. The surveillance operates in server-to-server space, beyond investigators' control or comprehension. For professionals whose work depends on discretion, the irony stings: the protection services have become the threat.

Adapting to Surveillance

Investigators now protect themselves from protection software. Jude avoids SSN searches when possible, reverting to "manual legwork" driving to county offices rather than risking automated searches. He still uses Delvepoint for vehicle records but understands the exposure risk.

The irony is complete: privacy protection services have become the surveillance network, alerting subjects when their information is accessed. The guardians are the watchers. No one watches them.

Author's Advice

By Lael Henterly CLI

It appears that an antivirus program, a browser extension or something in their browser such as Google Tag Manager is to blame. Microsoft Edge and Google Chrome's browsers are known to monitor activity in a manner similar to Avast. Delvepoint's website used GTM (Google Tag Manager), which can load secondary trackers invisibly. The site is likely passing users IP address, browser fingerprint, and referrer URL to Google and its ad partners, as well as behavioral metrics (page dwell time, clicks, queries, etc.) for marketing analytics. Many websites do this, we just don't normally notice beyond targeted ads.

To minimize data exposure when using any data broker with Google Tag Manager built in:

- Block Google Tag Manager and third-party scripts with uBlock Origin, NoScript, Privacy Badger, etc.
- Use a VPN to mask your IP.
- Visit data-broker or investigative platforms only in an isolated browser profile/ virtual machine.
- Clear cookies and site data after each session.

My advice would be stay as far away as possible from the identity protection products and avoid all browser extensions. One has only to look at every stock analyst review of these companies ever to note how misaligned their interests are with those of their customers. Their business depends on fears of identity theft and constant information leaks. To make smarter decisions about what to allow on your device, here are a few tips based on the Avast lawsuits:

Avoid Corporate Surveillance That Compromises Investigations

1. Don't trust "privacy" labels.

Avast sold itself as a shield against tracking while allegedly spying on users. Choose open-source tools that can be audited. Avoid extensions demanding full access to "read and change" web data.

2. Cut extensions.

Each add-on can act as a tap. Use your browser's native privacy tools. Disable or delete extras.

3. Keep data local.

Real privacy tools check sites locally rather than streaming your clicks to remote servers. Use browsers that filter threats on-device.

4. Isolate sensitive work.

Use a separate virtual machine or device for banking, health or legal matters.

5. Block cookies and scripts.

Avast used 45+ ad cookies. Block third-party cookies by default, clear data on exit, and run a strict blocker such as uBlock Origin.

6. Pay for privacy.

If the product is free, you're the product. Choose paid software that states plainly it doesn't sell data.

7. Monitor outbound traffic.

Use network monitors like Little Snitch or GlassWire. A trusted VPN or Tor adds another layer of identity protection.

8. Stay informed.

Privacy scandals often repeat. Check for regulatory actions or independent audits before installing anything.

Lael Henterly CLI founded Integra Intelligence, a boutique Seattle private investigation agency, in 2016. As a complex litigation investigator, she uncovers witnesses who substantiate white-collar crime allegations against corporate executives and public companies. Specializing in securities fraud, antitrust violations, corruption, and qui tam matters, In addition to being a CLI, she is a Certified International Investigator. She holds a journalism degree from the University of Washington and worked as an investigative journalist before transitioning to a career as a white collar crime investigator. She can be contacted at lael@integraitelligence.com