PRESS RELEASE

EMBARGOED UNTIL: April 6, 2026, 5:00 PM PST

Class Action Filed in California Federal Court Over LinkedIn's Ongoing Hidden Browser Scanning of US Users

Santa Monica, CA / Munich, Germany, April 7, 2026

A class action complaint was filed today in the US District Court for the Northern District of California by the Law Office of J.R. Howell on behalf of a proposed nationwide class. The complaint alleges that LinkedIn Corporation, a Microsoft subsidiary, runs a covert surveillance system inside the browser of every Chrome user who visits linkedin.com.

The system remains active today. On every page load, LinkedIn's code probes users' computers for thousands of browser extensions, scans the page for traces of additional extensions, and assembles a device fingerprint from dozens of hardware and software characteristics. The results are encrypted, transmitted to LinkedIn's servers, and reinjected into every subsequent request during the user's session. The code runs during CPU idle time, a concealment technique that reduces the chance a user will notice the scanning.

LinkedIn does not disclose these practices in its privacy policy. Users receive no prompt, no opt-in, and no indication that their computers are being interrogated.

The extension list is not limited to tools that scrape or automate LinkedIn. It includes religious extensions that identify a user's faith, political opinion extensions, tools built for neurodivergent users, and hundreds of job search extensions that expose whether someone is looking to leave their current position.

LinkedIn also routes session data to an undisclosed third-party company through a hidden zero-pixel iframe positioned off-screen. That company's public policies state it may integrate such data into its own products, share it with other clients, and use it for behavioral modeling and marketing. LinkedIn users are never told this channel exists.

The complaint brings six causes of action under federal and California privacy law, including violations of the Federal Wiretap Act and California's wiretapping and computer fraud statutes. It seeks compensatory and punitive damages, statutory damages of $5,000 per violation, and an injunction requiring LinkedIn to stop the scanning and delete collected data.

"This system can identify a user's religion, their political views, whether they have a disability, and whether they are secretly looking for work. LinkedIn knows every user's real name and employer. This is not abstract data collection. These are identified people being profiled without their knowledge," said J.R. Howell, attorney for the plaintiff and the proposed class.

Compliance or circumvention: why LinkedIn's scan list grew from 460 to 6,000 after EU regulation

In 2023, the European Union designated LinkedIn a gatekeeper under the Digital Markets Act, requiring it to open its platform to third-party tools through effective API access. Microsoft's response has been twofold.

In public, compliance theater. Microsoft published two APIs that do not provide access to core platform functions like direct messaging. Its 249-page compliance report to the European Commission mentions "API" hundreds of times but never once mentions Voyager, the internal API that powers LinkedIn's own products. Microsoft tells the Commission it cannot provide faster access. Voyager handles 14 billion calls per day. The API Microsoft offered to regulators handles roughly 6,000. That is a disparity of 2.25 million to one.

Behind the scenes, a different operation. While the Commission reviews compliance reports, LinkedIn expanded its scan list from roughly 460 entries in 2024 to over 6,000 by early 2026, including more than 200 products that compete directly with its own sales tools. The DMA gives businesses the right to build on LinkedIn's platform. BrowserGate identifies every company and every user who tries.

Microsoft's response

Microsoft has so far reacted by slandering the researchers who published the findings, calling the investigation a "smear campaign," and defending the scanning as necessary security measures.

Even though it is obviously irrelevant who first reported the findings, the researchers at Fairlinked would like to clarify two points.

Scanning for 6,000 extensions and transmitting the results to third parties without user consent is not server protection. It’s an illegal spying operation. The scan list contains thousands of extensions that have nothing to do with scraping. Religious extensions. Political opinion extensions. Job search tools. Neurodivergent aids. Amazon image downloaders. Pharmacy operations tools. Delivery schedulers. Clearly server protection is not the goal here.

The second is that the court case Microsoft cites has nothing to do with the surveillance operation. That case concerns an account suspension. BrowserGate was never mentioned in the proceedings. Microsoft implies it prevailed. It did not. A motion for a preliminary injunction was denied. Both plaintiffs have appealed. The litigation is ongoing. The fact that LinkedIn has

doxed the private home address of a Fairlinked member to the media speaks to the desperation of a company with no substantive defense.

The investigation and what comes next

The BrowserGate surveillance operation was published by Fairlinked e.V., Alliance for Digital Fairness, a newly founded nonprofit association of commercial LinkedIn users registered in Germany, representing businesses, professionals, and toolmakers who depend on the platform worldwide. The technical evidence is preserved with RFC 3161 qualified timestamps and supported by a sworn affidavit. BleepingComputer independently verified the scanning. LinkedIn has not denied any of the findings.

Fairlinked is coordinating with the Law Office of J.R. Howell on the US class action. In Europe, Fairlinked has filed complaints with the European Commission and is in regulatory dialogue with the Commission on what the market actually needs from LinkedIn's platform access. Fairlinked, which depends on donations and individual sponsors, is raising funds to enforce DMA regulation against Microsoft and end the compliance theater.

"LinkedIn's members are people and businesses who love the platform and invest heavily into it. We are here to hold Microsoft accountable and make LinkedIn accessible, so that users are protected from abuse and the millions of businesses and individuals who invest daily into the platform get their return on investment," said Steven Morell, a Board Member of Fairlinked e.V.

Media Contact

Steven Morell, President Fairlinked e.V. press@browsergate.eu browsergate.eu | fairlinked.eu