

LinkedIn, Microsoft, Persona, Biometric Identity Verification, Corporate Leadership, and Legal Risks to U.S. Citizens

Purpose

This document examines the relationship between LinkedIn, Microsoft, and Persona; the leadership and investment structures behind these companies; the use of biometric identity verification; documented privacy concerns; and relevant litigation.

The purpose is not to accuse any individual or company of criminal conduct without evidence. It is to identify documented facts and explain why the increasing use of private companies to collect and process government identification and biometric information can create legitimate privacy, cybersecurity, consumer-protection, and national-security concerns for U.S. citizens.

1. Who Owns LinkedIn?

LinkedIn is not an independently owned public company today.

Microsoft announced its agreement to acquire LinkedIn in June 2016 for approximately **\$26.2 billion**. The acquisition was completed on December 8, 2016. LinkedIn retained its brand and operated as a distinct subsidiary of Microsoft.

Microsoft's SEC filings confirm that it acquired all outstanding shares of LinkedIn Corporation.

Microsoft

Microsoft Corporation

Chairman and CEO: **Satya Nadella**

Microsoft is therefore the ultimate corporate parent of LinkedIn.

Satya Nadella is Microsoft's chairman and CEO.

LinkedIn

As of April 2026, **Dan Shapero is CEO of LinkedIn**. LinkedIn announced that Ryan Roslansky moved into the broader role of Executive Vice President of LinkedIn and Microsoft Office, with Shapero reporting to him.

Ryan Roslansky remains EVP of LinkedIn and Microsoft Office and is a member of Satya Nadella's senior leadership team.

The corporate chain is therefore:

Microsoft Corporation → LinkedIn Corporation → LinkedIn platform and services

2. Who Owns Persona?

Persona is a **private company**, rather than a publicly traded corporation.

Persona was founded by:

Rick Song

Co-Founder and CEO

Charles Yeh

Co-Founder and CTO

Persona's own investment announcements identify Song as co-founder and CEO and Charles Yeh as his co-founder.

Persona's publicly identified leadership also includes **Christie Kim**, **Duncan Sharp**, and **Neal Harris**. Rick Song publicly identified these individuals as Persona executives/leaders in 2026.

3. Persona's Major Investors

Because Persona is privately held, exact ownership percentages are not publicly available in the same manner as they would be for a publicly traded corporation.

However, Persona has publicly announced several major financing rounds.

Series B

Persona announced a **\$50 million Series B** led by **Index Ventures**, with participation from Coatue.

Mark Goldberg of Index Ventures joined Persona's board as part of that financing.

Series C

Persona subsequently announced a **\$150 million Series C** led by **Founders Fund**, with participation from:

- Founders Fund
- Meritech Capital

- BOND
- Insight Partners
- Index Ventures
- Coatue Management

The Series C valued Persona at approximately **\$1.5 billion** at the time.

Series D

Persona later raised another **\$200 million**, with the financing led by **Founders Fund and Ribbit Capital**. Mark Goldberg publicly described the round as a \$200 million financing led by Ribbit Capital and Founders Fund.

The publicly documented investment network therefore includes major venture-capital firms such as:

- Founders Fund
- Ribbit Capital
- Index Ventures
- Coatue
- BOND
- Meritech Capital
- Insight Partners

This is important because Persona is responsible for identity infrastructure used by major technology and commercial platforms, while the company itself remains privately held.

4. Persona Directors and Investors

Mark Goldberg

Mark Goldberg is associated with Index Ventures and joined Persona's board following Index Ventures' Series B investment.

Andy Chen

Andy Chen has been associated with Persona's board/director structure and has a venture-capital and technology background. He has publicly discussed his relationship with Rick Song dating back to Song's participation in the Kleiner Perkins Fellows program.

Rick Song

Rick Song is Persona's co-founder and CEO.

Charles Yeh

Charles Yeh is Persona's co-founder and CTO.

5. About the Chinese/Taiwanese Question

Some of the names associated with Persona may appear to be Chinese, Taiwanese, or otherwise East Asian to an English-speaking reader.

However, **a person's name does not establish nationality, birthplace, ethnicity, citizenship, political affiliation, or relationship to a foreign government.**

Accordingly, this document should not state that Persona's executives are Chinese or Taiwanese unless reliable biographical evidence establishes those facts.

There is currently no sufficient evidence establishing that Persona is controlled by the Chinese government.

That does **not** eliminate the legitimate national-security question.

The appropriate question is:

Who owns Persona, who has access to its systems, where is biometric information processed and stored, what foreign persons or entities have access to the company or its infrastructure, and what legal mechanisms could require disclosure of information?

Those questions can be investigated through corporate records, investment disclosures, privacy policies, contracts, subprocessors, data-storage information, and litigation.

6. What Persona Collects for LinkedIn

LinkedIn currently states that Persona collects certain personal information for its identity-verification process.

For Persona verification, LinkedIn says a user may be required to provide:

- A government-issued identification document
- A photograph of the identification document
- A selfie
- Information contained on the identification document

- A facial image used for identity verification

LinkedIn states that Persona is the party collecting certain personal data required for verification, including an image of the government-issued ID and a selfie.

LinkedIn states that it receives certain verification information from Persona, including the name appearing on the ID, the type and issuer of the ID, and Persona-generated identifiers.

LinkedIn says it **does not receive the user's biometric data or the photographs, numbers, expiration dates, or issue dates associated with the government ID.**

Persona's identity-verification system can nevertheless analyze facial geometry as part of the verification process.

7. Why This Creates a Risk for U.S. Citizens

Biometric information creates a different type of security problem than an ordinary password.

A password can be changed.

A person's face cannot.

If a password is compromised, a person can create a new password. If a biometric identifier is compromised, there is no equivalent process for replacing the underlying biological characteristic.

This makes biometric information particularly sensitive.

Potential risks include:

Identity theft

A combination of government identification, facial information, name, date of birth, and other identifying information can create a highly valuable identity profile.

Cybersecurity breaches

Any centralized collection of sensitive identity information can become an attractive target for criminals, hackers, intelligence services, or other malicious actors.

Insider access

Security risks do not exist only outside an organization. Employees, contractors, vendors, and subprocessors may potentially have access to sensitive information depending on the company's technical and contractual controls.

Third-party exposure

When LinkedIn uses Persona, information passes through a third-party identity-verification provider.

The individual therefore has to trust both LinkedIn and Persona, along with the relevant infrastructure and subprocessors.

Permanent biometric characteristics

Biometric identifiers cannot simply be reset like passwords.

Government access

Another important policy question concerns circumstances under which information held by a private company could become subject to legal process, government requests, subpoenas, warrants, regulatory demands, or other forms of compulsory disclosure.

Expansion of digital identity systems

As more online platforms require government IDs and biometric verification, private technology companies can become important intermediaries between citizens and access to digital services.

That raises a broader public-policy question:

Should access to ordinary online services or account recovery increasingly depend upon surrendering government identification and biometric information to private companies?

8. Documented Litigation Involving Persona

The existence of litigation does not mean that allegations were proven. The following cases should therefore be described as **lawsuits or legal proceedings involving allegations**, not as findings of wrongdoing.

1. Washington v. Persona Identities, Inc.

Illinois appellate litigation involving allegations under the Illinois Biometric Information Privacy Act.

The plaintiffs alleged that Persona's identity-verification system collected and stored facial geometry. The Illinois Appellate Court reversed an order compelling arbitration, holding that

Persona could not rely on an agreement between the plaintiffs and DoorDash to compel arbitration.

[Washington v. Persona Identities, Inc. — Illinois appellate decision](#)

2. Mouser v. Persona Identities, Inc.

Federal litigation involving Persona and alleged biometric/privacy claims.

The federal court ultimately remanded the case to Illinois state court after finding a lack of Article III standing.

[Mouser v. Persona Identities, Inc. — federal docket](#)

3. Parker v. Persona Identities, Inc.

A 2024 federal class-action complaint naming Persona.

The plaintiffs voluntarily dismissed the action without prejudice shortly after filing.

[Parker v. Persona Identities, Inc. — federal docket](#)

4. Freifeld v. Sonder Holdings Inc. and Persona Identities, Inc.

A federal class action alleging unlawful collection, use, storage, and disclosure of sensitive biometric information.

[Freifeld v. Sonder Holdings / Persona — federal docket](#)

5. Johnson, Mouser & Arman v. Persona Identities, Inc.

A federal action filed in the Northern District of Illinois in October 2024 naming Persona as defendant.

[Johnson et al. v. Persona Identities, Inc. — federal docket](#)

6. Speight v. Walmart, Inc., Persona Identities, Inc., et al.

A Connecticut federal case filed in November 2024 naming Persona, Rick Song, Walmart and other defendants.

The case was voluntarily dismissed shortly after filing.

[Speight v. Walmart / Persona — federal docket](#)

7. Persona Identities Inc. v. David Freifeld

Persona itself became the petitioner in a Seventh Circuit proceeding arising from the Freifeld litigation.

The appellate proceeding was docketed as **26-8016** in July 2026.

[Persona Identities Inc. v. David Freifeld — Seventh Circuit docket](#)

8. Peacock TV LLC v. Persona Identities, Inc.

This was a trademark proceeding before the U.S. Trademark Trial and Appeal Board rather than a biometric privacy lawsuit.

The TTAB entered a default judgment against Persona after no answer was filed, sustaining the opposition and refusing registration.

[Peacock TV LLC v. Persona Identities, Inc. — TTAB proceeding](#)

9. L.W.A. v. LinkedIn Corporation

This is a LinkedIn privacy case rather than a Persona lawsuit.

The plaintiff alleged that LinkedIn's Insight Tag intercepted private information from a third-party website. The court compelled arbitration.

[L.W.A. v. LinkedIn Corporation — federal decision](#)

10. Jackson v. LinkedIn Corporation

A LinkedIn privacy lawsuit concerning allegations that LinkedIn's Insight Tag obtained personal information associated with a California DMV website.

The court addressed claims involving the Drivers' Privacy Protection Act and California privacy law.

[Jackson v. LinkedIn Corporation — federal decision](#)

9. Additional LinkedIn Privacy Litigation

There are also multiple related LinkedIn cases involving the Insight Tag and health-related websites.

A 2025 federal court order identified four related putative class actions involving allegations that LinkedIn's Insight Tag collected information from health-related websites:

- **L.B. v. LinkedIn Corporation**

- **J.S. v. Spring Fertility Holdings, LLC**
- **V.R. v. LinkedIn Corporation**
- **J.P. v. LinkedIn Corporation**

The same court order noted three additional related cases, including L.W.A. and two cases filed in 2025.

[Federal court order discussing the related LinkedIn privacy cases](#)

10. LinkedIn's Broader Privacy Record

The biometric issue should also be viewed within the larger context of LinkedIn's data practices.

In 2025, LinkedIn faced a proposed class action alleging that it disclosed customers' private messages to third parties for purposes associated with training generative-AI models. Reuters reported that the plaintiffs alleged LinkedIn introduced a privacy setting in August 2024 and later updated its privacy policy.

LinkedIn has also faced litigation concerning its Insight Tag, including allegations involving health-related information and information collected from government websites.

These cases do not establish that LinkedIn or Microsoft unlawfully misused every category of information alleged in the complaints. They do demonstrate that **data collection, third-party tracking, privacy disclosures, and the use of personal information have repeatedly become subjects of litigation.**

11. What Can and Cannot Be Concluded

What can be established

LinkedIn is owned by Microsoft.

Microsoft acquired LinkedIn for approximately \$26.2 billion in 2016.

LinkedIn uses Persona for identity verification.

Persona collects government-ID information and selfies for its verification process.

Persona is privately held and backed by major venture-capital firms.

Persona's technology can process facial geometry as part of identity verification.

Persona and LinkedIn have been named in multiple lawsuits and legal proceedings involving privacy, biometric information, data collection, and related issues.

What cannot presently be established from the evidence reviewed

The available evidence does **not** establish that Persona is controlled by China.

It does not establish that Persona's executives are agents of the Chinese government.

It does not establish that a person's Chinese- or Taiwanese-sounding name means that person is Chinese or Taiwanese.

It does not establish that biometric information collected by Persona is being transferred to China.

Those claims would require additional documentary evidence.

12. The National-Security Question

The most important question is therefore not the ethnicity of the company's executives.

The more serious question is:

Who ultimately has access to the biometric and identity information of American citizens, where is that information processed and stored, and what legal, corporate, technical, or foreign relationships could provide access to it?

That question is appropriate because biometric identity systems can potentially affect millions of people.

The United States should require transparency regarding:

- Ownership
- Investors
- Board membership
- Foreign investment
- Data-storage locations
- Data-processing locations
- Subprocessors
- Employee access
- Contractor access
- Government requests
- Data-retention periods
- Security breaches

- Biometric deletion procedures
- Cross-border data transfers
- Secondary uses of biometric information

Conclusion

The use of biometric identity verification by major online platforms presents both legitimate benefits and legitimate risks.

Persona may help LinkedIn prevent fraudulent account access and impersonation. At the same time, the process can require citizens to place highly sensitive government-identification information and facial information into the hands of a private third-party company.

The appropriate public-policy question is therefore not whether every person involved in these companies should be viewed with suspicion.

It is whether **American citizens have sufficient legal and technical protections when private technology companies become intermediaries for government identification and biometric identity.**

Biometric information is uniquely sensitive because it is intrinsically connected to the individual.

A password can be changed.

A face cannot.

For that reason, biometric systems used at scale should be subject to exceptionally strong security, transparency, retention, consent, and national-security safeguards.

Source: <https://piunikaweb.com/2026/02/23/persona-ceo-faceless-linkedin-profile-debate-x/>

Source: [https://en.wikipedia.org/wiki/Persona_\(identity_verification_service\)](https://en.wikipedia.org/wiki/Persona_(identity_verification_service))



May 10, 2023
12pm PT / 3pm ET

Mark Goldberg
Index Ventures
Rick Song
Persona



TECHBLITZ

デジタル世界でも
「顧客を知る」方法

persona

Co-Founder and CEO
Rick Song



INNOVATOR



RICK SONG

**President
@Brand Innovators**

**ICONS, ROCKSTARS, & INNOVATORS
CELEBRATE AAPI EXCELLENCE**



Ask a 
fintech
founder

VISA

