What public breaches actually show about who controls your data

Public incidents show that data risk extends past the company you chose, to its credentials, employees, contractors, dependencies, connected devices, and legal obligations.

Abstract

A review of public breach disclosures, regulator actions, government reports, company notices, and AI privacy documentation shows a recurring pattern: when data is held or processed outside a user's direct control, the security and privacy boundary expands to include more systems, more people, more credentials, more dependencies, and more legal obligations. This does not prove that hosted infrastructure is inherently unsafe. It does show why ownership, explicit permissions, data location, portability, and controlled connectivity are meaningful product properties rather than marketing ones.

Key findings

- Third-party custody expands the number of systems and people that can become part of a data incident.
- A cloud-hosted data incident does not require the underlying cloud provider itself to have been breached.
- Connected devices can turn cameras, microphones, and vehicles into ongoing sources of sensitive behavioral data.
- AI conversation records can be sensitive data, and can also become subject to legal process when a provider holds them.
- User-controlled infrastructure reduces some third-party exposure, but does not remove the need for layered security, recovery, updates, and careful permissions.

Methodology

I worked from primary sources: regulator actions and final orders, securities filings, government cybersecurity bodies, company incident disclosures, and provider privacy documentation. High-quality independent reporting was used only where it added confirmation or legal context. Every example is classified by what kind of evidence it actually is, so that a confirmed breach, a regulatory allegation, a final order, a company disclosure, a software failure, a provider policy, and a court process are never treated as the same thing.

Limits

This is a curated set of public incidents, not a complete census, and it was assembled to test a specific question about custody and control. It does not measure how often these failures happen, it does not compare the security performance of any two named companies, and it does not establish that one infrastructure model is categorically

safer than another. A larger or differently selected sample could change the emphasis, though the classification rule would still apply.

Sources

- HHS: Change Healthcare cybersecurity incident FAQ
  https://www.hhs.gov/hipaa/for-profession als/special-topics/change-healthcare-cybersecurity-incident-frequently-asked-que stions/index.html
- AT&T Form 8-K on the third-party cloud workspace incident
  https://www.sec.gov/Archives/edgar/data/ 732717/000073271724000046/t-20240506.htm
- CERT-EU analysis of the European Commission supply-chain incident
  https://cert.europa.eu/blog/european-com mission-cloud-breach-trivy-supply-chain
- FTC case against Ring
  https://www.ftc.gov/news-events/news/pre ss-releases/2023/05/ftc-says-ring-employees-illegally-surveilled-customers-faile d-stop-hackers-taking-control-users
- Wyze incident update on the thumbnail failure
  https://forums.wyze.com/t/update-on-inve stigation-of-2-16-24-security-issue/2910 02
- FTC final order involving GM and OnStar
  https://www.ftc.gov/news-events/news/pre ss-releases/2026/01/ftc-finalizes-order-settling-allegations-gm-onstar-collected -sold-geolocation-data-without-consumers
- UK ICO fine against 23andMe
  https://ico.org.uk/about-the-ico/media-c entre/news-and-blogs/2025/06/23andme-fined-for-failing-to-protect-uk-users-genet ic-data/
- UK ICO on protections during the 23andMe sale
  https://ico.org.uk/about-the-ico/media-c entre/news-and-blogs/2025/05/ico-calls-for-protections-for-23andme-customer-data /
- LastPass security incident update
  https://blog.lastpass.com/posts/notice-o f-recent-security-incident
- Coinbase Form 8-K on insider-assisted access
  https://www.sec.gov/Archives/edgar/data/ 1679788/000167978825000094/coin-20250514 .htm
- Live Nation Form 8-K on the third-party cloud database
  https://www.sec.gov/Archives/edgar/data/ 1335258/000133525824000081/lyv-20240520. htm
- Snowflake Form 10-Q on customer account access
  https://www.sec.gov/Archives/edgar/data/ 1640147/000164014724000207/snow-20240731 .htm
- OpenAI on business and API data commitments
  https://openai.com/business-data/
- OpenAI statement on the request for consumer ChatGPT conversations
  https://openai.com/index/fighting-nyt-us er-privacy-invasion/
- Google Gemini Apps Privacy Hub
  https://support.google.com/gemini/answer /13594961?hl=en
- Reuters on the DeepSeek database exposure
- Reuters on the 2026 chatbot records warrant ruling
- Odido security update on the voice-phishing incident
  https://www.odido.nl/veiligheid