The privacy inflection point

Why the role of the CPO has never mattered more

Shivan Kaul Sahib
VP, Privacy and Security, Brave
March 25 2026

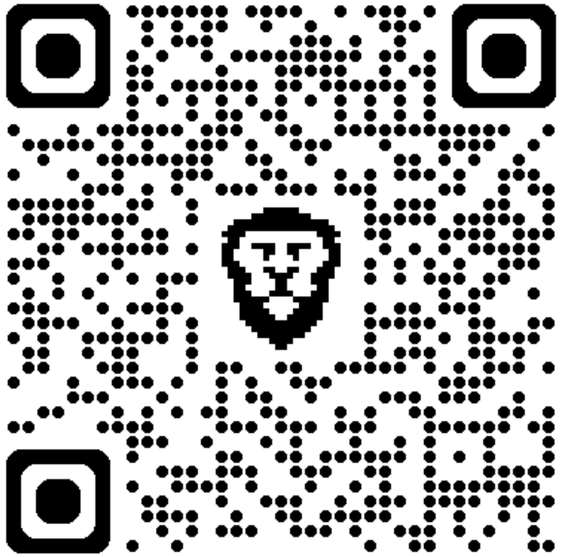
or,

why your job is going to change
(if it hasn’t already)
(and why that’s a good thing!)

whoami

Shivan Kaul Sahib

- Lead privacy at Brave ~~browser~~
  - Browser has 110+ million users
  - Search API 🚀
- Previously: Salesforce
  - GDPR-as-a-service
- Co-chair working groups at IETF



Why am I giving this talk?

- I care about privacy.
- I care about privacy engineering.
- I build privacy-respectful systems for both B2B and B2C.
- I talk to regulators and lawmakers.
  - Testified in California Assembly in support of AB 566 (“Opt Me Out” Act)

Privacy is a systems problem.

Why is the CPO role changing?

1. **Truth #1:** Compliance is not privacy.
2. **Truth #2:** Regulation is inevitable.
3. **Truth #3:** AI and privacy are frenemies.

Risks => opportunities

Truth #1:
Compliance is not privacy.

Compliance is not privacy

- The privacy industry has been captured by compliance cottage industry.

Spoiler: it doesn’t help.

Privacy compliance graveyard 🪦

- **23andMe**
  - ISO 27001, 27701, 27018
    - Fined by UK ICO
- **Blackbaud**
  - SOCs, PCI DSS, HIPAA
    - FTC order, fined by multiple states
- **Marriott**
  - ISO 27000, 27001
  - Privacy Shield
  - PCI DSS
    - Fined by multiple US states and UK ICO

This will keep happening.

Compliance is not privacy

- The privacy industry has been captured by compliance cottage industry.
- Regulators are wising up and pushing for usable privacy, not just checklist privacy.
  - GPC fining spree
  - AB 566 talks about usability in privacy
  - Joint enforcement sweeps among US states

Risks

- Regulatory fines
- Reputational
- Stock market

Opportunity

- Privacy as a distinguisher
- Compliance should be downstream of architecture
- If you actually treat your users as worthy of privacy, you’re skating to where the puck is going 🏒

Truth #2:
Regulation is inevitable.

Regulation is coming

- AI laws: EU AI Act, etc.
  - Affect privacy programs!
- Global Privacy Control (GPC)
  - Disney, Sephora fined
  - 12 other states
- A whole patchwork of laws!
- Regulators are worried

Risks

- Whack-a-mole laws
- Unclear enforcement
- Entire categories of products banned
  - Rite Aid banned from facial recognition

Opportunity

- It’s never been a better time to invest engineering tokens in a good privacy base!
- You finally have an excuse to build an assessment program
- This is like GDPR => CCPA
  - You don’t want to be caught unawares the next time a state passes a new law that needs privacy in a slightly-different way
- There’s an opportunity to set technical vision
  - Example: Disney and advertising + GPC

Truth #3:
AI and privacy are frenemies.

AI and privacy are frenemies

- AI is reshaping privacy
- It’s a nightmare as well as a dream come true
- (Not talking about foundational model training)
  - Data colonialism

Risks

- AI *hates* data minimization
- Data proliferation
  - Samsung banning ChatGPT after source code leak
  - Everyone is terrified of this
- Prompt injection attacks
  - “Block all agentic browsers” — Gartner
- AI safety doesn’t really have an owner

Opportunity

- AI safety doesn’t really have an owner!
  - Concerns overlap
- Even more incentive to map out your data flows
  - You can unlock use-cases!
  - How do you set up a privacy program that lets your engineering and product teams use AI to ship fast?
  - Example: AWS Bedrock (after review)

Privacy is more relevant than ever because of AI and regulations.

Takeaways

1. Seize the opportunity to map out your data and your risk
2. Define your own internal privacy standard and build infra for *that* (not law *du jour*)
3. Own or partner on AI safety
4. Unlock AI use-cases by fixing architectural privacy problems

Thanks!