“You have zero privacy anyway. Get over it!”

- Scott McNealy, 1999
Highest Penalties in Privacy Enforcement Actions

$148 M  States v. Uber

$230 M  British Authority v. British Airways (proposed)

$275 M  CFPB and States v. Equifax

$5,000,000,000
FTC v. Facebook

Source: Federal Trade Commission | FTC.gov
Privacy-by-design Framework

1. Proactive, not reactive
2. Strong default settings
3. Embedded into, not bolted on
4. Positive-sum
5. E2E security
6. Openness and transparency
7. Respect for the user

Ann Cavoukian, Image licensed under CC from Wikimedia Commons
Simple enough concepts; paired with explosion of privacy tooling in the last decade...

So why are we here?
We know what “good” programs look like

Don’t we?

- Triage questionnaires
- PIAs
- DPIAs
- Policy approvals
- Exceptions
- Risk assessments
- Vendor reviews
- Certifications
- Audits
- etc.
Common pitfalls of privacy processes

- Lack of visibility and access → Can’t fix what you don’t see
- Lack of resources → Only 24 hours in a day
- Politics → Avoid being the “blocker”
- Clash of cultures → “Process” = delay = less “impact”

These issues are especially acute in small & rapidly growing organizations
The single most impactful thing you can do as your company’s “privacy person” is turn everyone else into a “privacy person” too.
Keep a checklist for yourself

- Policies
- Data maps
- Records of processing
- Security assessments
- DSARs
- All the rest...

Focus on culture; Ask questions

- Why does privacy matter?
- What are our principles?
- What could go wrong?
- What more can go right?
- What do our users expect of us?
- What can you, as the product manager, engineer, designer teach me?
How to build a “privacy-by-ethos” culture

- Make it fun
- Start early
- Be consistent; be present
- Invite conversations
- Real-life rewards work
- Use what’s already there to your advantage