When Engineers and Lawyers Talk: Right-sizing your Data Protection Risk Profile

Rafae Bhatti
Director of Security and Compliance, Mode

LinkedIn: rafaebhatti
Twitter: @privacyphd
Who Am I?

I build data protection programs at startups

I am also a licensed CA attorney
What This Talk is About?

Right-sizing the risk profile
Parallax

So an engineer and a lawyer walked into a bar...
Data Protection Risks

- Data subject expectations
  - Collection
  - Processing/Sharing
  - Retention

- Data protection safeguards
  - Security controls
  - Contractual obligations

- Adequate/reasonable
  - Risk acceptance
Right-Sizing Examples
Let's Go!

Risk scenarios ahead
Scenario 1

A company retains personal data of consumers for analytics purposes.

A CA resident asks them to “Delete all data you have about me” under CCPA.

Can the company keep the analytics data?
CCPA Exemptions
Data Retention

Takeaway

- Retention is tied to purpose of use
- Consider if the purpose is internal use or helps with security audit or troubleshooting
- Consumer expectations and context when collected
Scenario 2

A company’s vendor launches an email campaign using the personal data of the company’s users.

The data belongs to consumers in CA.

Can a CA consumer sue the company for a CCPA violation?
CCPA Sale: Example
Vendor Data Use

Takeaway

● Audit data use for vendor with PII, including cookie scan

● In addition to legal commitments, use tools (such as plug-ins) to protect personal data

● Tie vendor security to business consequences
Scenario 3

A company accidentally shares a report belonging to organization A with organization B.

The data belongs to consumers in the EU.

Is the company required to notify the consumers of a data breach?
Clarity in Uncertainty

Video: Sully Movie CLIP - Brace for Impact (2016) - Tom Hanks Movie
Data Breaches: Clarity in Uncertainty

Find your unique profile to calibrate risks

1. Exposed data included personal data
2. Exposed data was not encrypted
3. The source of breach has not been addressed

Under CCPA -> Enough to decide
Under GDPR -> Consider high risk
High Risk Processing?
Data Processing Risk

Takeaway

- Degree of risk is a matter of data subject expectation
- Mandatory code review when high level of risk in processing data
- Tie risk of disclosure to business consequences

Different analysis for CA and EU
Understanding Risks Has its Rewards

Security Roadmap
- Communicate security risks
- Translate risks into needs
- Create security culture

Tooling and Scaling
- Privacy Engineering
Conclusion

Be prepared for how to avoid a bad situation or prevent it from getting worse

When it’s our time to land:
Hope we are on the Hudson, not in it.
Thankyou!

LinkedIn: rafaebhatti
Twitter: @privacyphd