May 10, 2024

Game of Thrones Meets Modern Family: Building a Practical Privacy Program

Dave Cohen
LevelUP Consulting Partners

Peter McLaughlin
Rimon, P.C.

Elise Houlik
Intuit

Dean Forbes
DaVita

Privacy+ Security Forum

Speakers

Privacy+ Security Forum

Dave Cohen

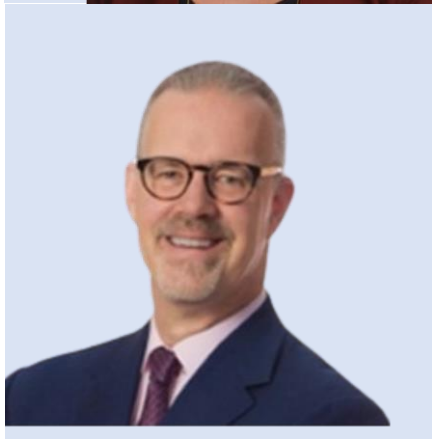
Director
LevelUP Consulting Partners

Elise Houlik

Chief Privacy Officer
Intuit

Dean Forbes

Vice President, Associate General Counsel, Chief Privacy Officer
DaVita



Peter McLaughlin

Partner – Data Privacy & Security
Rimon P.C.

Where does the Privacy Legal Line End and the Operational Line Begin?

- The roles between legal and operational privacy advice are blurry at best.
- How do you ensure your program is legally compliant and operationally achievable?
- When do you call outside counsel versus consultants?
- How do you make effective use of legal and ops in program development and maintenance?
- What factors should you consider while managing organizational risk and liability?

Privacy+ Security Forum

Agenda

I. Welcome and Introductions
II. Privacy Program Maturity Level (Polling)
III. Laying out the Premise – Discussing Considerations
IV. Examples of a Privacy Program Structure
V. Operational and Legal Working Together
VI. Hypothetical Scenario/Audience Examples
VII. Questions and Answers

Privacy Program Maturity Level/Size

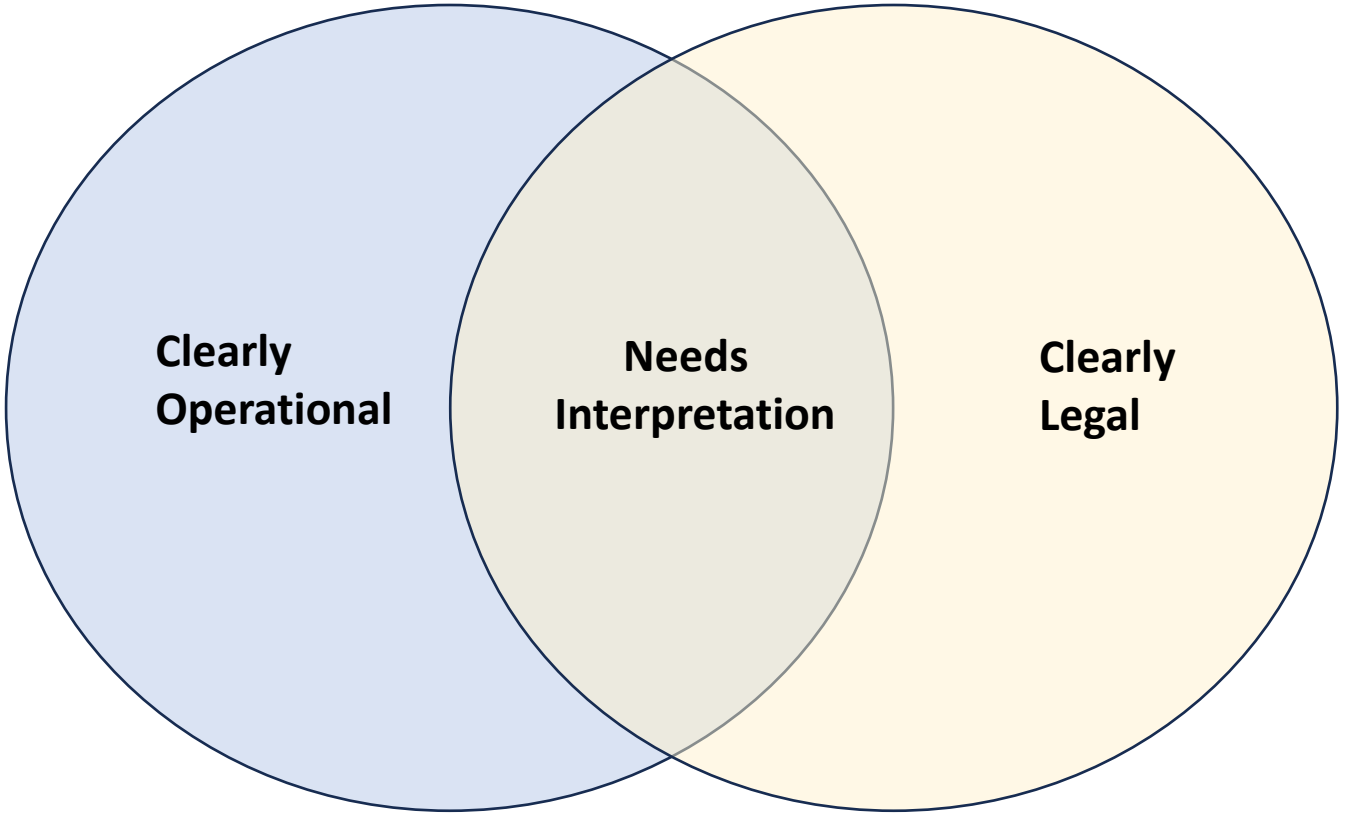
Privacy+ Security Forum

1. **By a show of hands, how would you rate the current maturity level of your privacy program?**
    a. Initial building stages, just getting started.
    b. A basic operational program is in place, we are seeking to enhance our efforts.
    c. We have a mature program and are looking for ways to increase efficiency and effectiveness.
2. **Would you characterize your privacy program as small, medium or large?**
    a. Small = 1 - 5 person staff dedicated to privacy
    b. Medium = 6 – 20 person staff dedicated to privacy
    c. Large = Over 20 person staff dedicated to privacy

Overview – The Need for Multiple Perspectives

Privacy+ Security Forum

Privacy program decisions are often complex and should be viewed through legal, business, risk and operational lenses.



Example of a Privacy Program Structure

Privacy Program's Purpose:

- Help the company to be thoughtful about how it collects, uses and shares data
- Help the company drive innovation and growth through responsible data use
- Help the company understand how privacy can enhance products/services, and drive a competitive advantage

Example of Enterprise Privacy Program Structure / Governance

Privacy+ Security Forum

Privacy Program Management	Privacy & Cybersecurity Legal	Privacy Engineering	International Privacy and Data Protection
Program and Project Management	Tracking external legal requirements	Privacy-by-Design (PbD) program	Coordinates with country privacy leads
Policies and Procedures; Risk Assessments; Data Use Review; DSARs	Day-to-day legal advice (to business and Privacy Team)	Application requirements and collateral support	Local Policies and Procedures; Training; Risk Assessments; ROPAs
Training and Communications	Vendor privacy and cybersecurity due diligence; Contracting support	Application logging and monitoring (ALM)	Coordinates with US team on enterprise privacy issues (e.g., global privacy policies)
Cross-department committees	Coordinate with IT/ IT Security; advise on technology adoption legal issues (e.g., AI)	Data loss prevention (DLP)	Coordinates with US team on int'l M&A, cross-border data transfers, IR matters
Metrics	IR Management	Data inventory and data mapping	Coordinates with US team on PET use

Operational and Legal Working Together

Privacy+ Security Forum

So, can we talk? Let's discuss some ways in which legal and ops can (and importantly, have) worked together to move projects forward.

And since it's not unusual for each side (well, the outside providers at least) to want to do a larger part of the pie, how does the organization's legal and/or privacy leadership manage this?

Hypothetical Scenario

Privacy+ Security Forum

A large B-C company operating in the United States, Europe and South America has decided to simplify their consumer rights policies and procedures to provide universal rights of access, correction and deletion for all customers regardless of jurisdiction.

Understanding this is a simplified scenario,

1. What are some operational advantages and disadvantages to this approach?
2. What are some financial advantages and disadvantages involved?
3. What are some legal compliance and risk issues involved?
4. Any other pros and cons to this approach over the alternative of providing consumer rights only to those from jurisdictions where they are legally obligated?

Additional Scenarios – Who Ya Gonna Call?

Privacy+ Security Forum

1. You know you have WA state consumers using your health app, but what does the law require that is different from your HIPAA obligations?

2. Where is our data and how do we best manage consumer requests?

3. We need help developing policies, procedures, and internal mechanisms to ensure that we fulfill our obligations

Questions & Contacts

Privacy+ Security Forum

Dave Cohen

dave.cohen@levelupconsult.com
(603) 498 1121

LinkedIn

Dean Forbes

dean.forbes@davita.com

LinkedIn

Elise Houlik

LinkedIn

Peter McLaughlin

peter.mclaughlin@rimonlaw.com

LinkedIn