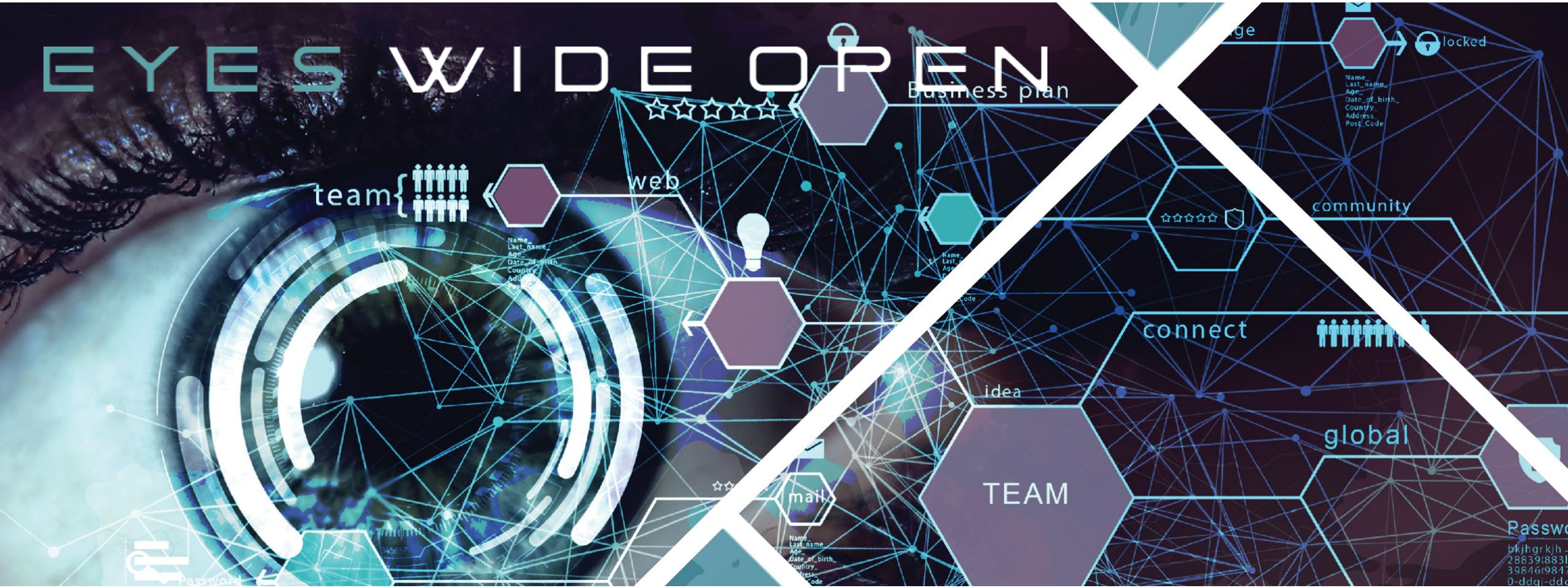
12TH ANNUAL LEADERSHIP EVENT

CYBER SECURITY SUMMIT

Security solutions through collaboration.™

TITLE SPONSOR

Island



The Intersection of Privacy and Security:

How you can use Existing Security Tools to Build an Adaptive Privacy Program

About Me

<u>Present:</u>

Privacy Consultant/ GC

<u>Past:</u>

Deputy CISO

Lawyer

TRUVANTIS®

Disclaimers

- My views
- For educational purposes
- Not legal advice
- Privacy is BIG, this presentation is small (i.e. high level)
- My answer to your question is “It depends”

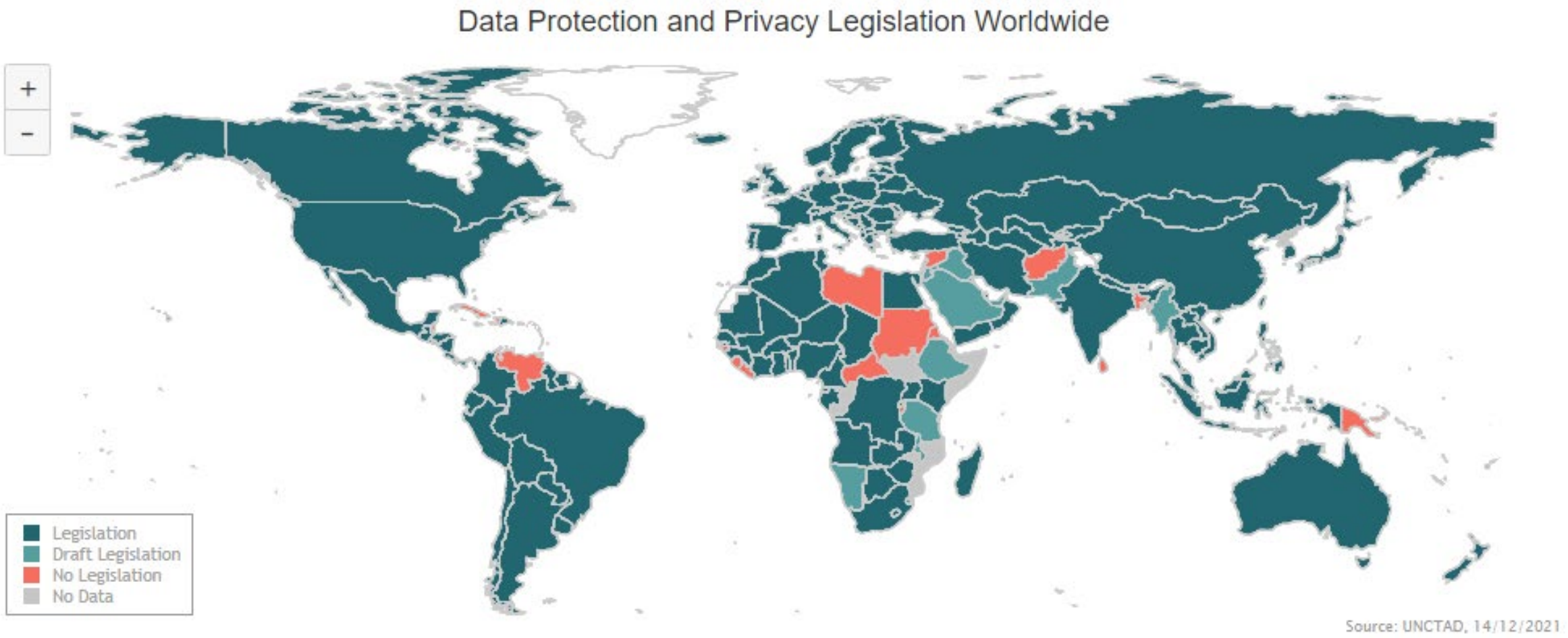
3 Questions I'd Ask at This Point:

- Should I stay for this?
- Privacy isn't my job, why should I even care?
- What time is the break?

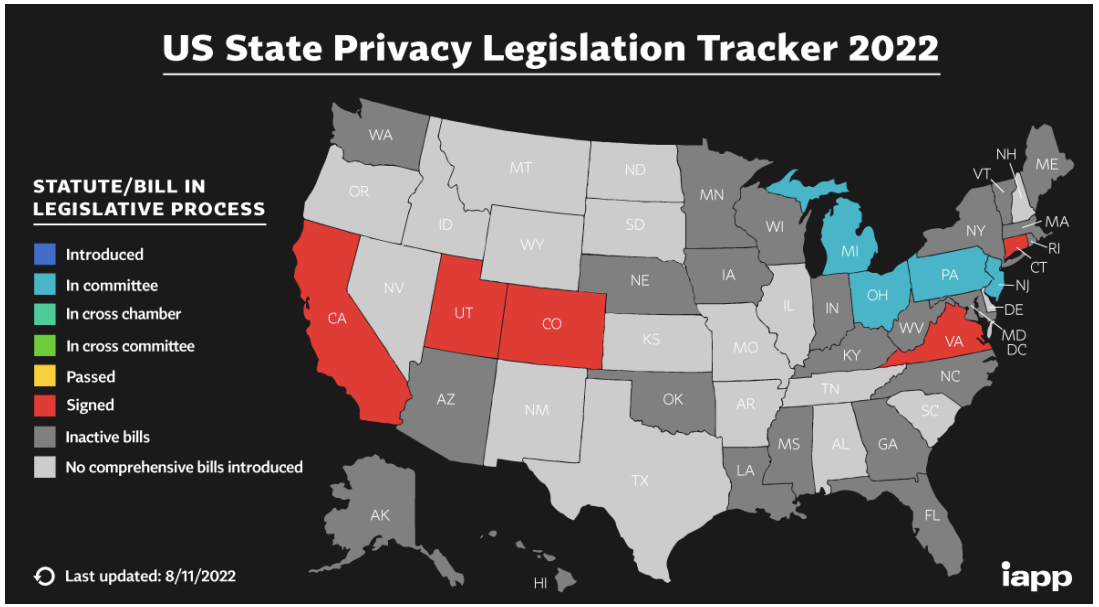
Takeaways

- Privacy and cybersecurity are the same
- Security is the foundation of a good privacy program
- Combined risk leads to adaptability

Global Privacy Footprint



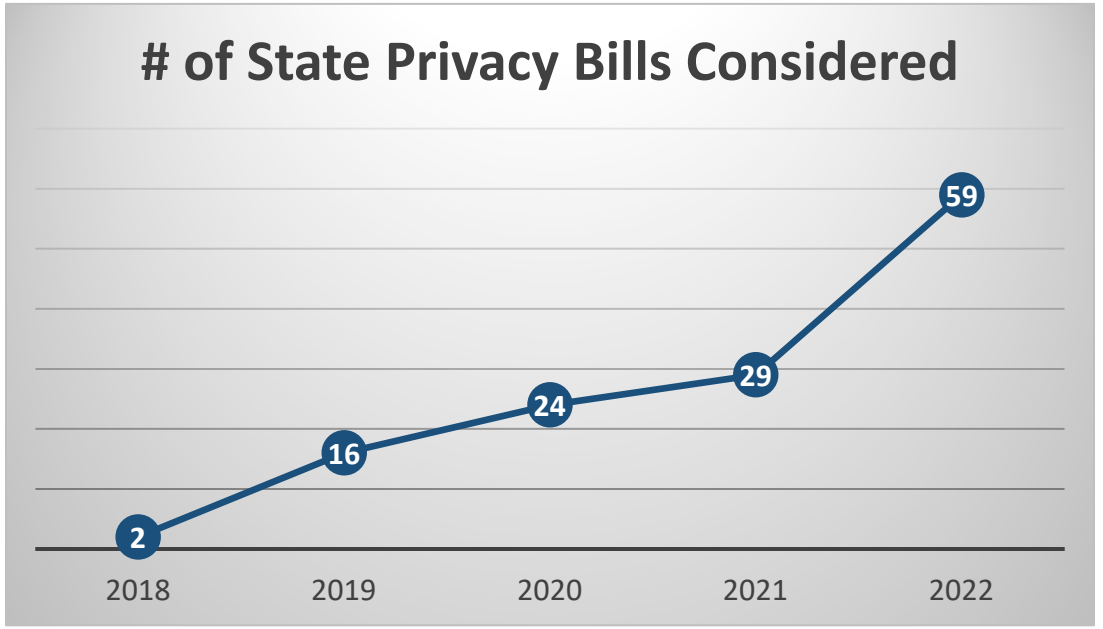
US Privacy Footprint



Source: https://iapp.org/media/images/resource_center/State_Comp_Privacy_Law_Map.png

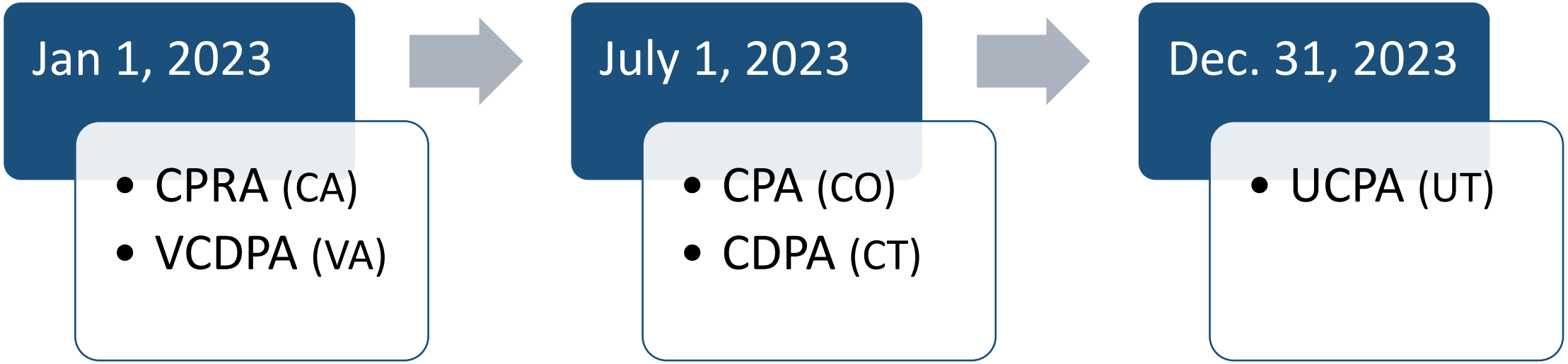
- All 50 States have data breach notification law
- 5 have comprehensive privacy laws

- Significant increase in legislative activity 2018 to 2022



New Comprehensive US Privacy Laws

Effective Dates for Comprehensive Privacy Legislation



Individual Privacy Rights

	Right to Access	Right to Correct	Right to Delete	Right to Portability	Right to Opt out of all or specific processing	Right to Opt in for sensitive processing	Age based opt in right	Right not to be subject to automated decision making
GDPR								
CCPA (CA)								
CPRA (CA)								
CPA (CO)								
CDPA (CT)								
VCDPA (VA)								
UCPA (UT)								

Security Related Business Obligations

	"Reasonable Security"	Privacy Risk/ Impact Assessments
GDPR		
CCPA (CA)		
CPRA (CA)		
CPA (CO)		
CDPA (CT)		
VCDPA (VA)		
UCPA (UT)		

US Privacy Regulators- Sample

Federal

State

Enforcement Actions Examples

	BLU Products 2018	LabMD 2016	Shein/ Zoetop 2022	Sephora 2022
Enforcement Body	FTC	FTC	NY Attorney General	CPPA
Violation	Deceptive Practices -Misrepresented extent of info shared and security practices	Unfair Practices -failing to take appropriate measures to prevent unauthorized disclosure of sensitive information	Deceptive Practices - Failing to have reasonable security; failure to disclose	CCPA Violation -improper "sale" of information
Remedy	Cease inappropriate practices and implement comprehensive security program	Initially, comprehensive security plan, but overruled by 11th Cir. Ct App. Separate settlement followed.	Comprehensive security plan. Prescriptive measures, i.e. risk assess, annual reviews, more.	Clarify notice, enhance opt- out (GPC), conform to CCPA, report to AG

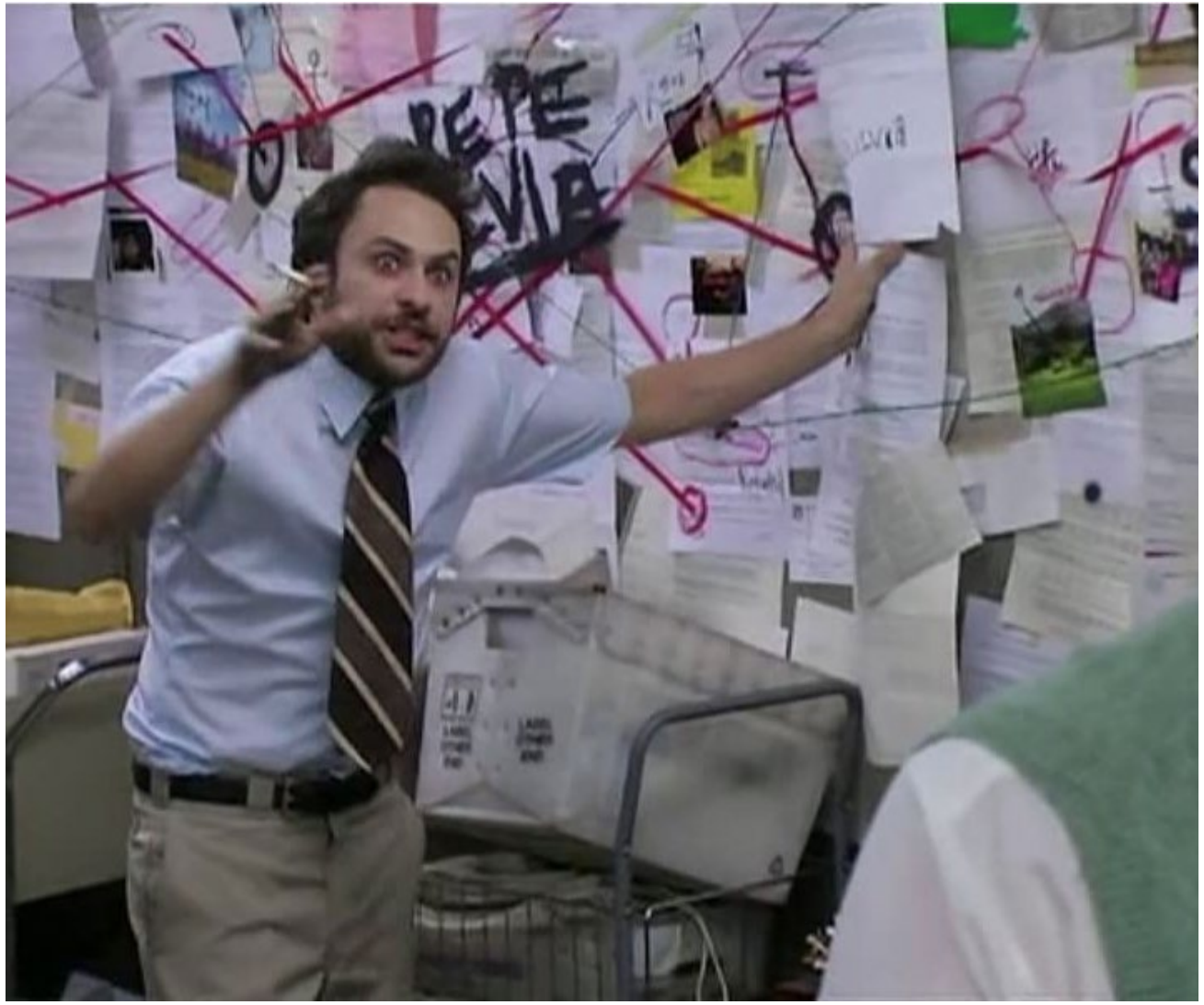
Prescriptive Requirements Example

FTC Requirements in Ashley Madison case (2016):

- Written Security Plan
- Training
- 3rd Party Security
- Monitoring
- Unsuccessful Login Tracking
- Remote Access Controls
- Encryption Key Storage
- Secure Passwords
- Password Retention

How can you use existing security tools to build an adaptive privacy program?

1. Alignment of stakeholders
2. Combined Privacy and Security Risk Assessment
3. Repeatable process for continuous monitoring



Source: https://www.imdb.com/title/tt1290725/mediaviewer/rm3459106561?ref_=ttmi_mi_all_sf_3

1. Align Key Stakeholders

Legal	Security	Privacy
• Strong organizational influence • ID applicable laws • Interpret key terms	• Strong knowledge of security risk and assessment • Also knows baseline controls for protection	• Develops business practices for managing covered data • Lead for incident response and data inquiries

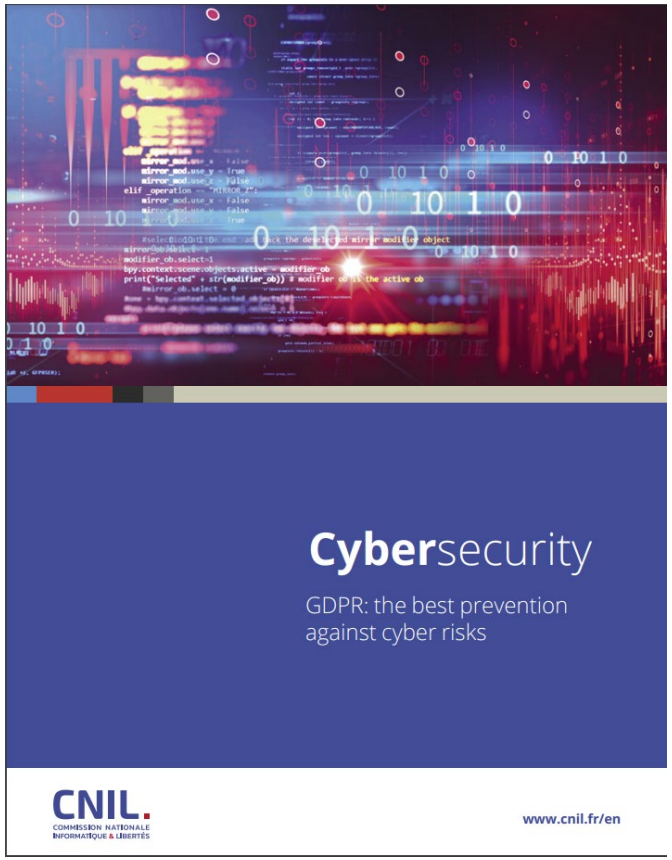
Discovering Convergence

"While they require different knowledge bases, privacy and security go hand in hand. Effective data privacy is impossible without robust security measures."

Source: thtps://iapp.org/media/pdf/resource_center/iapp_isc2_white_paper_next_generation_security_privacy_professional.pdf

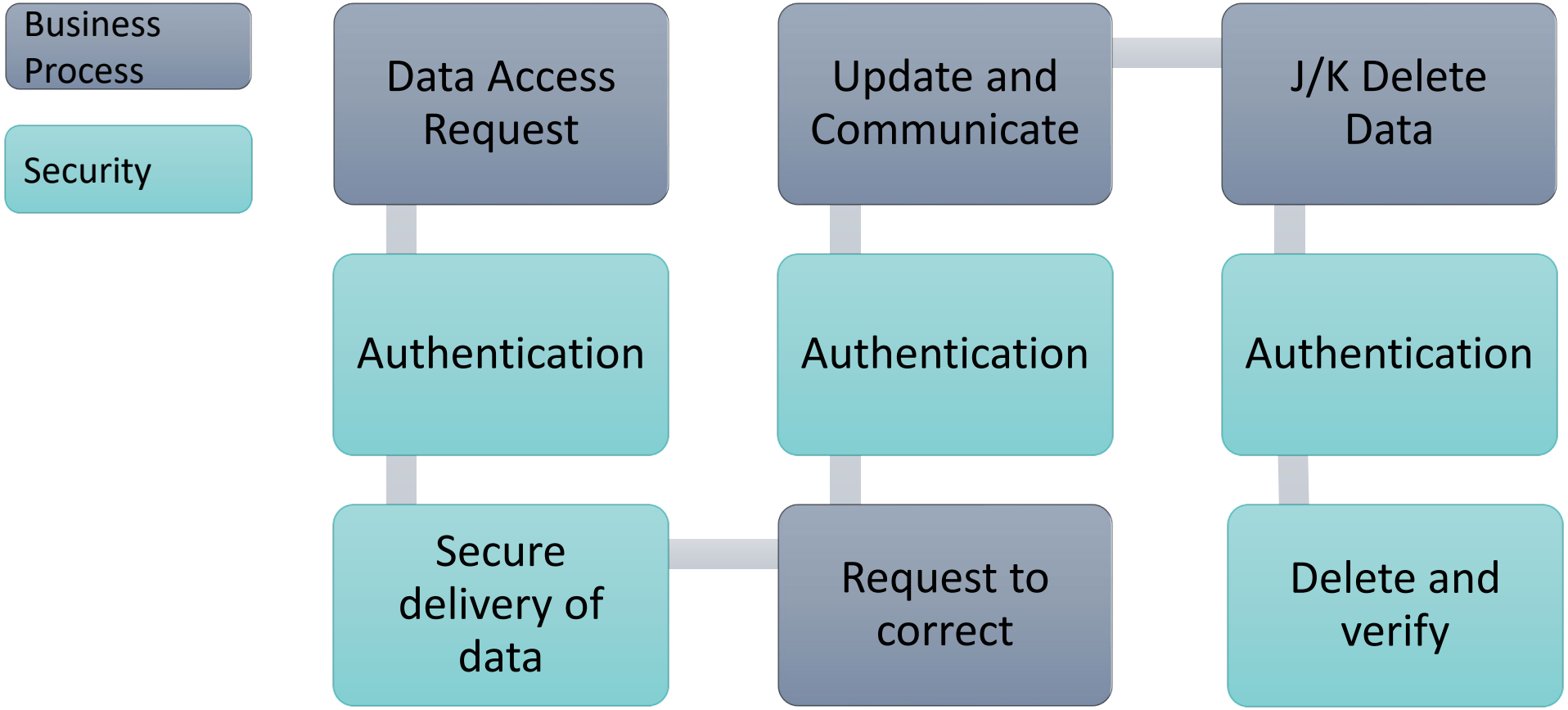
Global Trend

- “The multidisciplinary approach is a necessity; there can be no data protection without security”

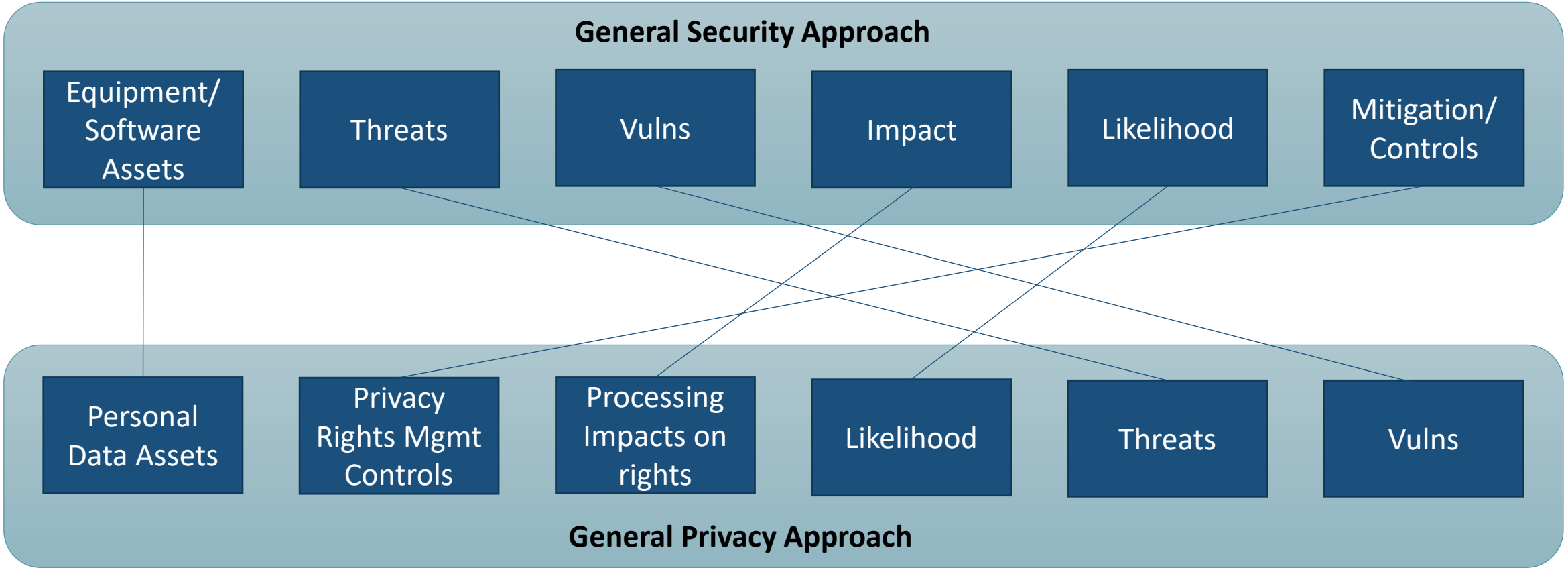


https://www.cnil.fr/sites/default/files/atoms/files/cybersecurity-2021_gdpr-the-best-prevention-against-cyber-risks.pdf

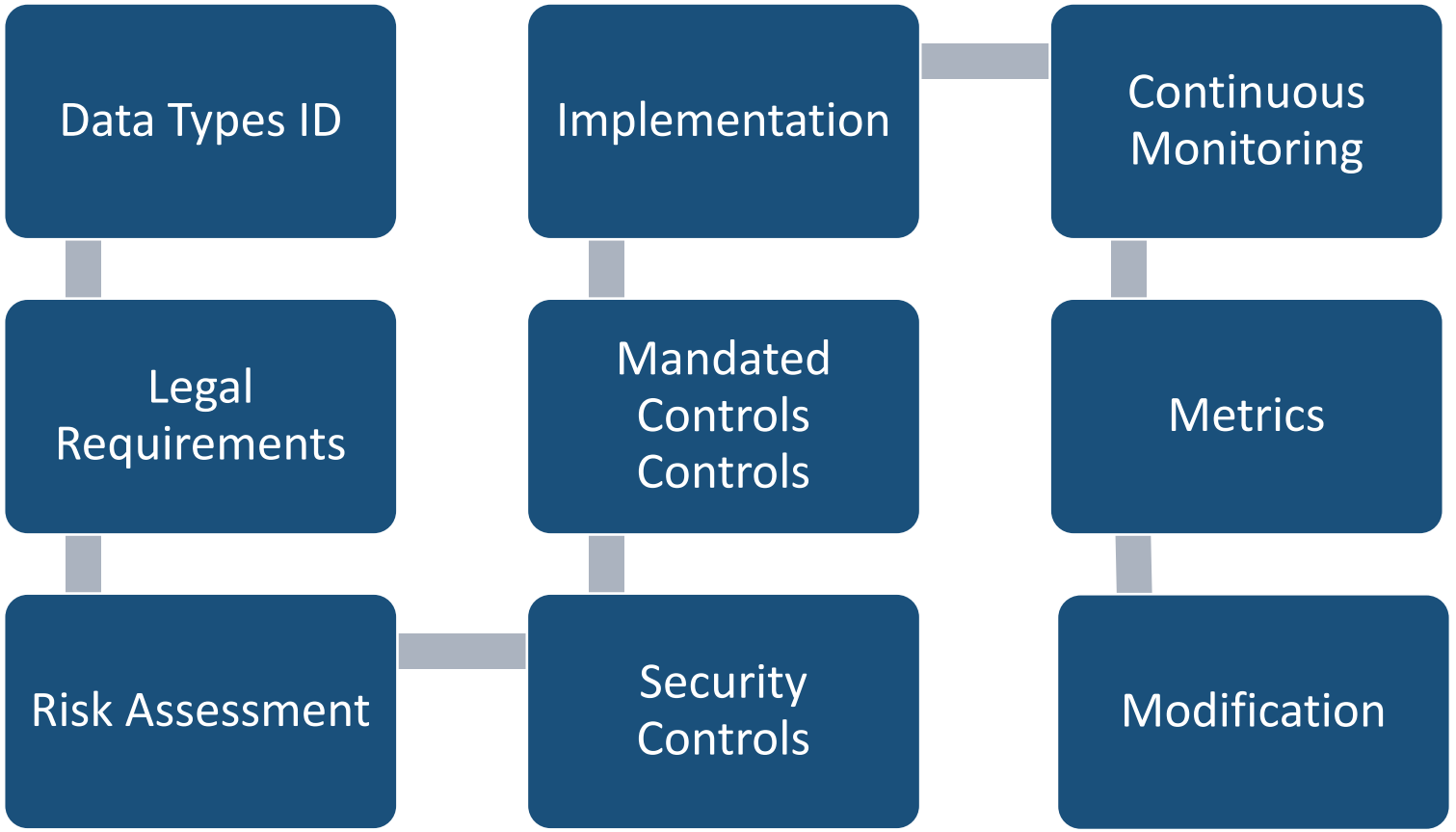
Example: Privacy/Security In Practice



2. Combine Security and Privacy Risk

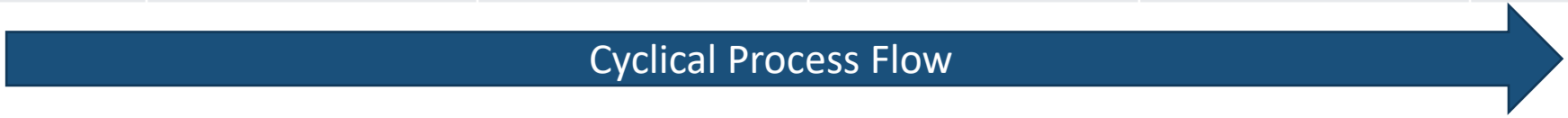


Combined Model Components



Combined Risk Model

	Asset	Threat	Vulnerability	Impact	Likelihood	Mitigation
SCOPE	• Data focused • Inventory • Map data flow • ID Business process/ processing activities	• Threats to data • Threats to data subject rights	• Weakness in data flow or business process • Threat event or scenario development	• Business Impacts • Consumer or Individual Impacts	• Probability	• Treatment • Controls ID • POA&M
FUNCTION	• Legal • Privacy • Security	• Privacy • Security	• Privacy • Security	• Legal • Privacy • Security	• Privacy • Security	• Legal • Privacy • Security



3. Repeatable Process

- Be able to repeat assessment upon significant change
- Change in technology, business process, law, etc.
- Cross reference risk register

Adapting to Change

Importance of Ethics

- 1970's Ford Pinto Example:
  - Ford knew risk of exploding gas tank
  - Cost to fix: $137.5 Mil
  - Cost if do nothing: $$49.5 Mil
  - Ford did nothing
  - Grimshaw v. Ford Motor Company, 1981
- Privacy relevance
  - Don't use risk analysis to justify bad business decisions

Source: https://www.tortmuseum.org/ford-pinto/#images-2

Emerging: Secret Life of PETs

- Privacy Enhancing Technologies (examples)
  - Homomorphic Encryption
  - Secure multi-party computation (SMPC)
  - Differential Privacy
  - Zero-knowledge proofs (ZKP)
  - Obfuscation
  - Psudonymization
  - Communication anonymizers
  - Synthetic data generation
  - Federated learning

Thank You!

Truvantis is a cybersecurity & privacy consulting organization with comprehensive experience in implementing, testing, auditing, and operating cybersecurity and information privacy programs. We specialize in helping our clients improve their cyber governance posture through practical, effective, and actionable programs — balancing security, technology, business impact, and organizational risk tolerance.

Jerrod Montoya, JD, CIPP-US

(855)345-6298

Sales@truvantis.com

TRUVANTIS®