CSNP

PRIVACYSWAN
CONSULTING™

January 25, 2023

PRIVACY**SWAN**
CONSULTING™

GSLC · iapp OFFICIAL TRAINING PARTNER · CIPT · CIPM · CIPP/E · PMP

Janelle Hsia

CISA Certified Information Systems Auditor

20+ years spanning Technology – Security – Privacy

- Principal Privacy and Data Protection Training and Consulting
- Director of Privacy and Compliance for SMB
- Deputy Information System Security Officer in the DOC
- Past Board of Directors for CSA Colorado Chapter
- ISSA Privacy Special Interest Group Tri-Chair
- IEEE Digital Privacy Committee
- IOPD Founding Board Member
- Not a lawyer ☺

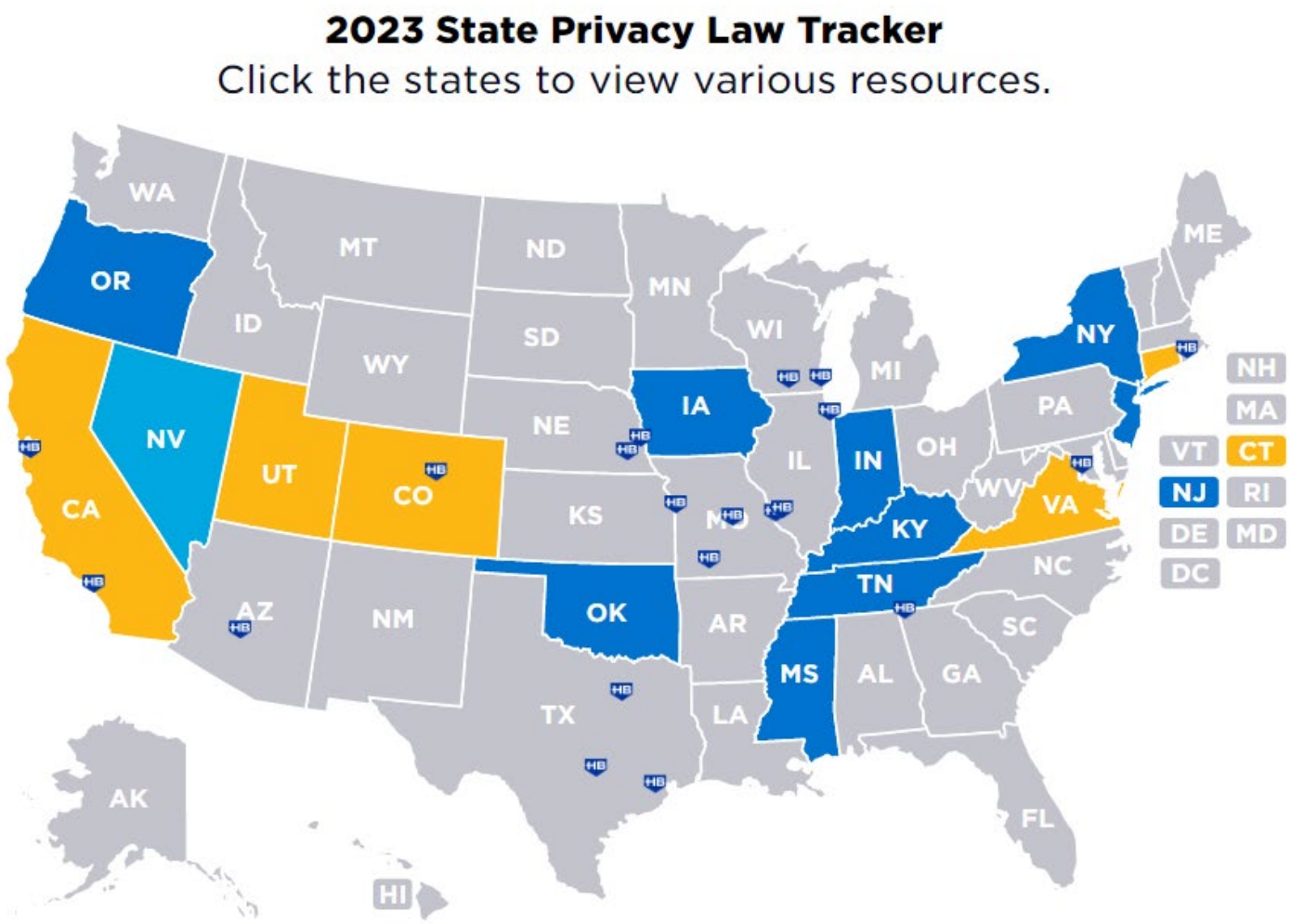
Services

- Privacy Training
- Privacy Program Development
- Strategic Privacy by Design
- Privacy Risk Analysis
- ISO 27701 & NIST CSF with Privacy
- GDPR
- CCPA/CPRA
- CPA (Colorado)

The dirty little secrets

in privacy

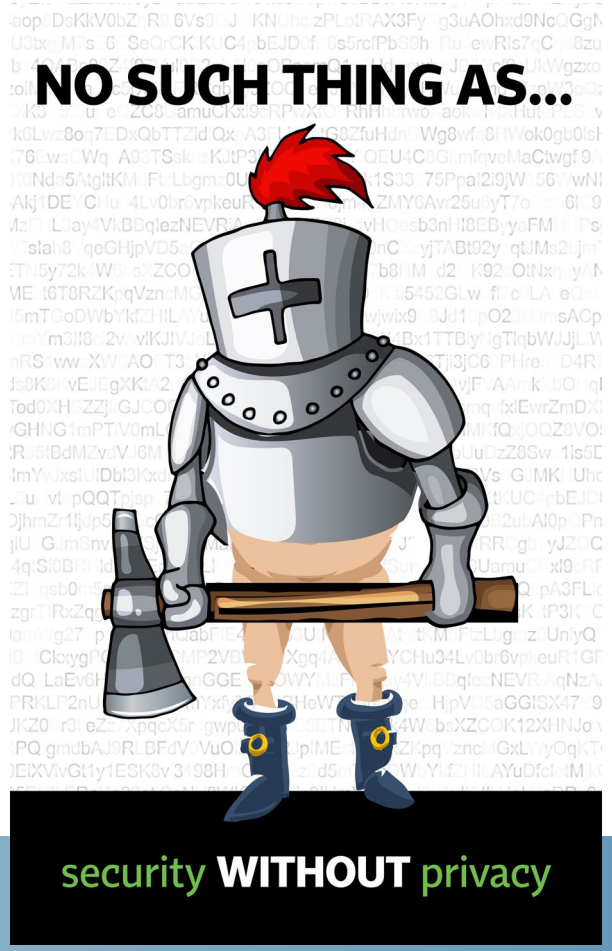
US Legal Landscape



https://www.huschblackwell.com/2023-state-privacy-law-tracker

Privacy is...


NAUGHTY
NICE
GDPR
VIOLATION
EST.
2018
ARTICLE 4
iapp.org


NO SUCH THING AS...
security WITHOUT privacy

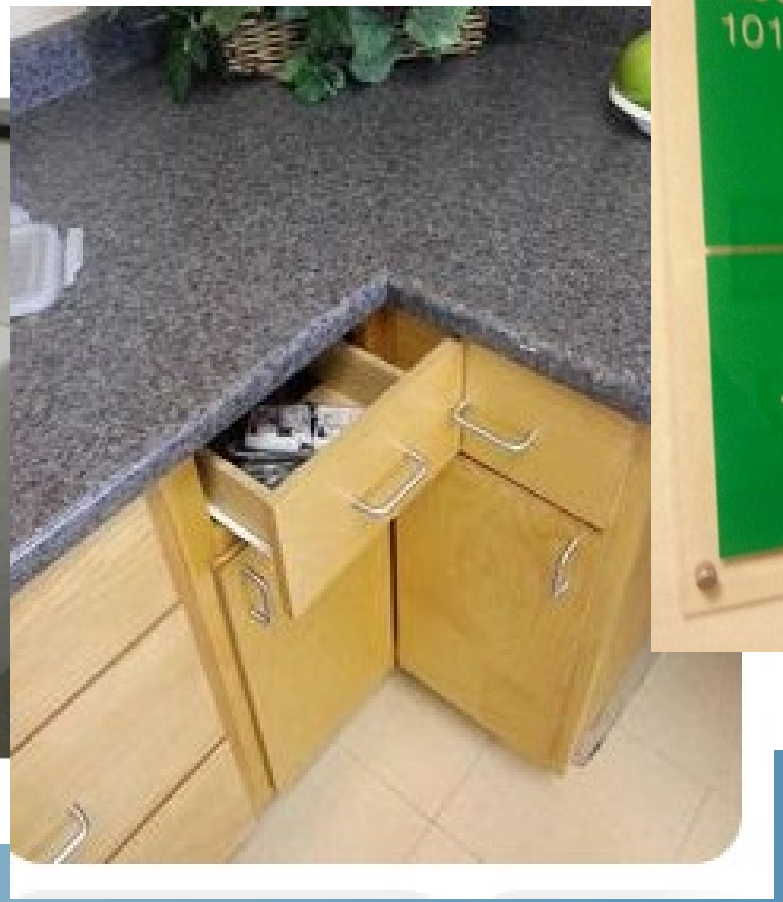

DATA?
I don't have to show you any stinking data.
iapp.org

All about…

- Data Subject Requests
- Data Minimization
- “Reasonable” Security
- Risk Assessment – DPIA/PIA
- Breach Notification
- No Dark Patterns

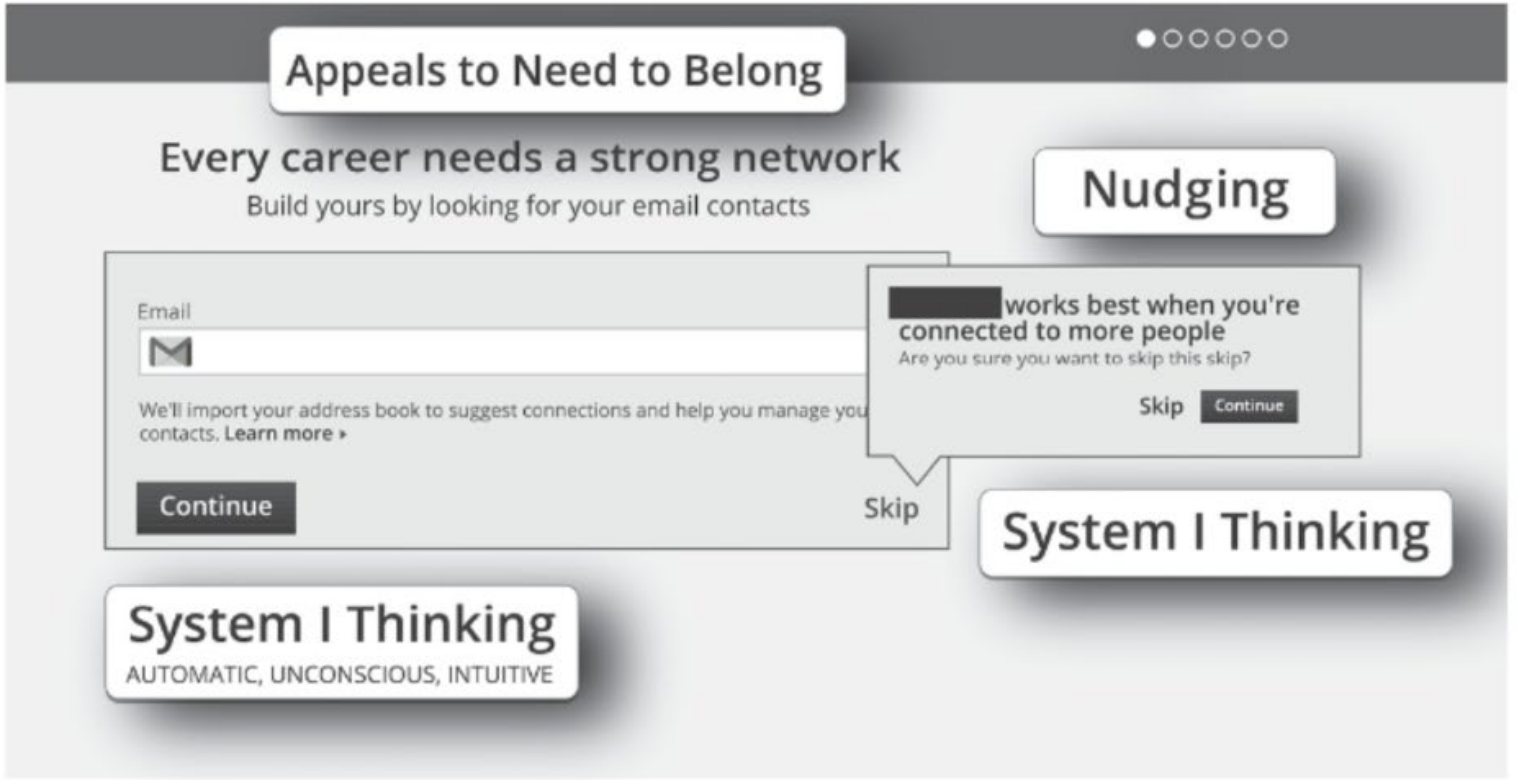
We need to fix Bad Design...

Source: Ryan Kaverman



Design shapes how we see things

- Design choices
- Automation
- Micro-targeting



Strategic Privacy by Design - R. Jason Cronk

Why do **WE** have a problem?

The burden should be on the organization and not on the individual:

- organizations are the ones collecting the personal data and they are the only one that know how they will use the data
- privacy notices and ‘choice’ don’t work

Is it really a choice?

✓ Yes, please add me to your list!

Would you like to receive additional information?

✓ Yes
○ No

❑ Click here to unsubscribe

The default is YES
Opt-out

❑ Yes, please add me to your list!

Would you like to receive additional information?

❑ Yes
❑ No

❑ Click here to subscribe

The default is NO!
Opt-in

It's all about the data

Know where the data is located

Data is like Water

Just start … it's a process

Data Inventory

ROPA Record of Processing Activities

Start somewhere
Start small

Just Start!!

Where to look

- Asset and/or System Inventory
- Development and Test Systems
- Vendors
- Reports
- Old Data and Storage
- Shadow IT and Unauthorized SaaS
- Finance

It has a source

Collection

Create

Internal to the organization

External to the organization

Acquire

Active – direct – openly – aware - transparently

Passive – indirect – secretly - unaware

Repurpose (Secondary Use)

Data collected for one thing but used for other thing

And a destination

Vendors

- If company credentials (email address, username) are used
- If it is purchased with company resources (credit card or PO)
- Even if it is FREE but you are using it to do your job
- If you are transmitting ANY kind of company related information to, with, or from it

It doesn't just disappear

Retention and Destruction

Retention requirements

DSR – right to be forgotten

Delete it – really delete it

- Encryption Key Shredding
- Degaussing
- Destroying
- Shredding
- Archive
- Mark for Deletion

NIST 800-88 Guidelines for Media Sanitization

It's still only about the data

Incident Response

What are privacy incidents?

Only legal uses the "B" word

What is an incident?

If in doubt, shout it out

See something, say something.

How to report an incident?

Email phishing button

security@yourcompany.com

Don't include attachments

Taking into account the...

state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk

RISK to the person regarding their DATA

Not all risks are the same

A Privacy Impact Assessment (PIA)/Privacy Threshold Analysis (PTA) looks at the risk (surveillance, invasion, aggregation, disclosure) of processing an individual's personal data.

It is concerned with the individual not the organization and takes into consider the impact to the individual.

Moving from PTA – PIA - DPIA

Looking for the TIGERs in the organization

Employees can be our ~~biggest weakness~~

greatest strength

Build a culture of privacy and security

Employees

- Stop and think about it
- Verify the person they are sharing personal data with
- Don’t use business data for personal reasons
- Email is not a document repository
- Credential management

Privacy Leader

- Set the tone for personal data processing
- Privacy strategy
- Understand organizational risk
- Laws and Regulations

(GDPR/CCPA/CPRA/CPA/VDPA)

Privacy Champions

- Understand privacy
- Understand the use of personal data
- Understand the harm to the person
- Spread the word
- Boots on the ground

Why should you care?

Systems contain data about people not just personal data

What should you do?

1. Think differently
2. Build a Privacy Program
3. Work together
4. Learn about Strategies and Tactics
5. Learn about PETs

Resources

Conferences

- https://www.petsymposium.org/cfp23.php
- https://www.usenix.org/conference/soups2023
- https://www.usenix.org/conferences/byname/1046 - PEPR
- https://iapp.org/conference/iapp-privacy-security-risk/

Organizations

- https://iapp.org/
- https://noyb.eu/en
- https://fpf.org/
- https://epic.org/
- https://www.eff.org/

Privacy by Design

- https://instituteofprivacydesign.org/
- https://www.iso.org/standard/76772.html
- https://privacybydesign.training/
- http://cs.ru.nl/J.H.Hoepman/publications/pds-booklet.pdf

Resources

PRIVACYSWAN CONSULTING™

Janelle Hsia

Janelle@PrivacySWAN.com

Thank you