SHARE
EDUCATE ‣ NETWORK ‣ INFLUENCE

Managing Compliance in the Wild West of Converging Data Security and Privacy Policy

Colin Oakhill | Management Consultant, InSoft Software GmbH, Germany

Tony Perri | CEO, Perri Marketing, Chattanooga, Tennessee

infotel
Insoft-Infotel.com

perrimarketing

Who is Infotel?

Established in 1979 the Infotel brand is global:

- HQ Paris with offices and subsidiaries in France, Germany, the Netherlands, United Kingdom, USA, Canada, India and Morocco
- Software division "InSoft Infotel" based in France & Germany
- Business partners around the world
- More than 100 persons dedicated to R&D in 3 labs
- 730 clients worldwide in 45 countries
- Expertise in products and utilities for Db2 for z/OS & LUW, smart data remediation, electronic archiving, digital preservation, and records management
- 1st product world-wide for aircraft technical documentation

Who is Colin Oakhill?

- Management Consultant at InSoft Software GmbH, Germany
- Started career in 1972 after studying Mathematics & Computer Science in UK.
- Programming experience started with technical applications in Fortran and Assembler for an Operations Research solution and 8-bit assembler for military applications.
- Continuing through to designing and programming database optimization software for z/OS systems in Assembler.
- Well known in the DB2 world, having vast experience in many various database systems such as IMS, Total and IDMS. Deep operating systems experience in z/OS and CICS systems.
- Founded the company "InSoft Software" in 1986 and designed / created several successful products.

First general release of DB/IQ Quality Assurance was in the mid 90's.

Who is Tony Perri?

- 1980 - started in college as Fortran programming student
- Transferred to creative writing. Took off from school until 1988 to schlep food.
- Mid 1990s - started in the s/w biz after a long stint in foodservice
- 2008 - began working in mainframe space at Allen Systems Group
- 2011 - Founded PMI, a tech marketing company, in 2011

  Current/past clients: BMC, Cloud Compiling, CorreLog, DTS Software Eccox Software, **Infotel,** KoolSpan, SyncDog, Redwall Technologies, SysperTec, Zetaly (zCost)
  Here this week representing Infotel

- Over the years many research/technical writing projects in InfoSec space
- IBM Champion 2022-2024
- Co-founder and CEO of Santa Rosa Software, a mainframe small s/w vendor specializing in mobile applications for next-gen mainframers

Agenda – Taming the ‘Data Cowboys of The Wild West’

1. Potentially “Bad” Actors and Their Silos
2. The “broken playing field” in large enterprises
   a) Regulations plus data: toxic gold
   b) Compliance and IT, Marketing, HR, and other core business units working in silos
   c) Data everywhere with accesses unknown
3. Relationships and Opportunities
   a) Frenemies, internal customers, and perspectives
4. What do we do about all this to identify where the data is to maintain security and compliance?
5. Discussion

The Actors Exposing Data Compliance Risk

CEO and the Board

- They set the strategy and let others worry about the details
- Results today are more important than consequences tomorrow

CMO

- Messaging! Reputation! Revenue! Brand Strategy! Exclamation Marks!!!!
- Abstract role in organization – misunderstood, hard to measure, seen as a cost center

CTO and/or CIO

- Totally different people with totally different jobs, not at all interchangeable
- At least one of them reports to the CEO unless they report to the CFO
- Responsible for technology and business impact, maybe also vision
- Abstract roles in organization – misunderstood, hard to measure, seen as a cost center

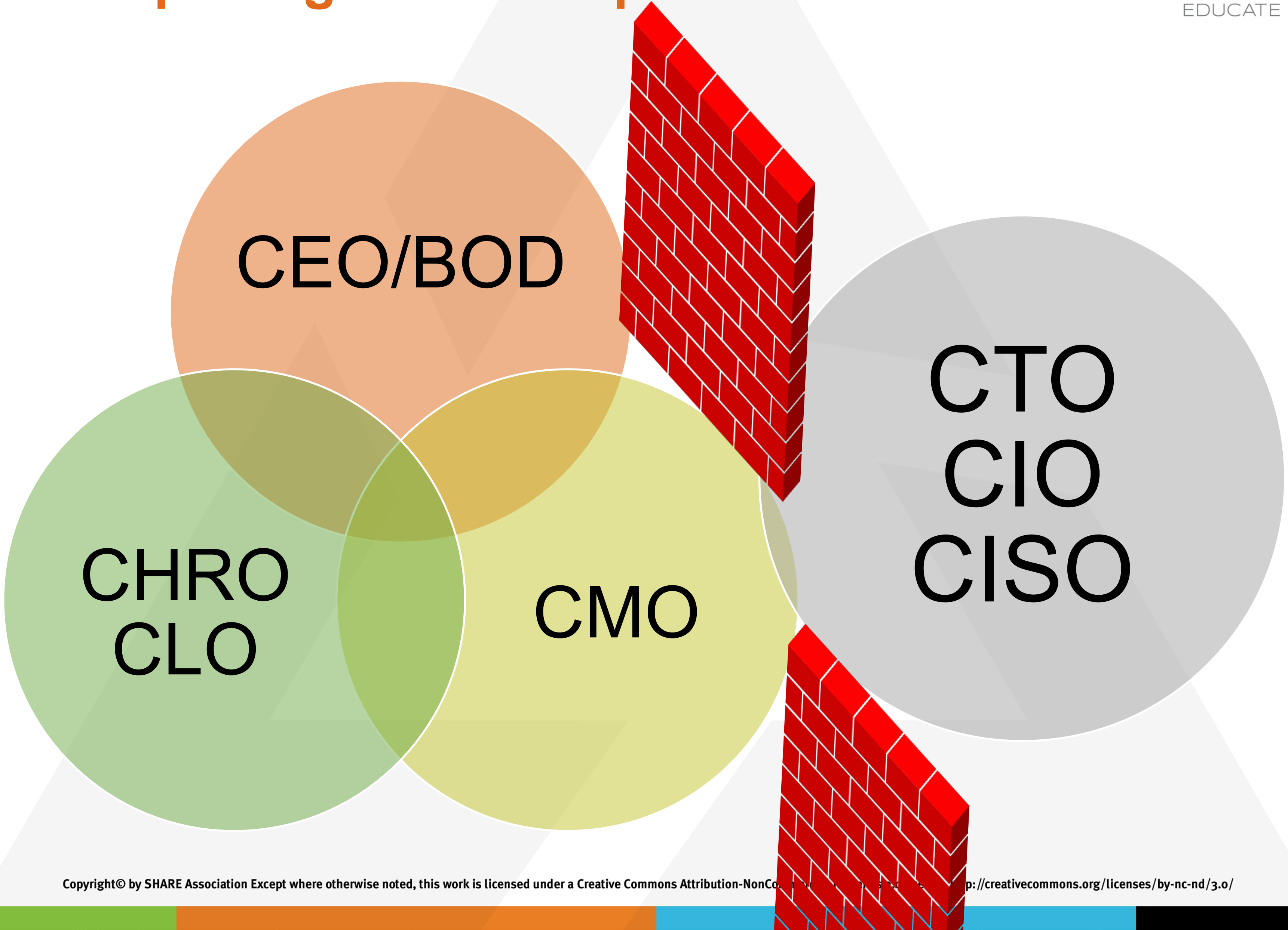
CHRO/CLO

- "Human Resources" – squeezing the business value out of headcount
- "Just keep us out of trouble"…

CISO

- When everyone else ignores the security and regulatory implications, the shouting sound comes from here

The Actors Exposing Data Compliance Risk



The Same Silos You Deal With

- **The line of business:** either a super silo, or the value other silos fail to “get”
- **IT:** shepherding the bits and bytes, keeping tech current, keeping dissatisfaction within SLA QoS
  - Even “insiders” often don’t have the whole picture of their own silo
- **Marketing:** the strategic face the organization shows the world
- **Human Resources:** keepers of the parameters for people
- **Legal:** the parameters setters
- **Internal customers:** they keep the boat afloat and rocking
  - Putting the “cuss” in customer
  - Forcing you IT folks to triage if there are conflicting demands
- **Audit and Data Security:** the ultimate inside outsiders

So What?

- The focus of all organizations with mainframes (revenue in $billions) is to stay out front and on top, shareholder value
  - Much (if not all) the software is commoditized. If you are a marketer, data is the differentiator!
  - Many marketing and ops leaders are in charge of data in your org. How well do you think they know security, privacy and compliance?
  - They must grow the business within constraints of regulations, compliance, data security, insurability, liability

- How do you maintain your organization’s viability when it takes an army working together to be successful
  - But silos of people are just trying to keep their head above water.

The ‘Why’ and the Opportunities

SHARE
EDUCATE ‣ NETWORK ‣ INFLUENCE

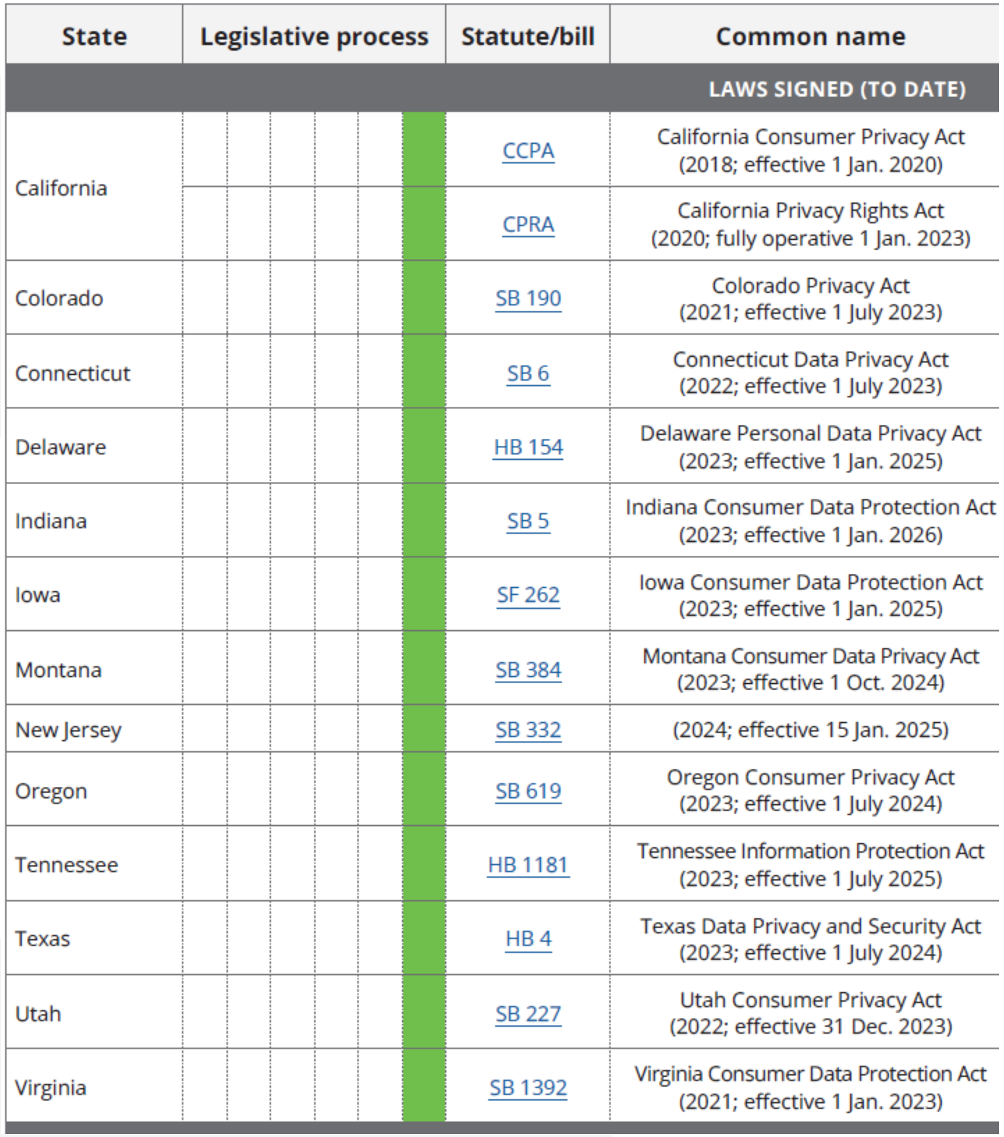
- DATA PRIVACY VIOLATION TO LAWS/REGS IS DEVASTATING!
  - The biggest data breach fines, penalties, and settlements so far (September, 2023)
    - Didi Global: $1.19 billion
    - Amazon: $877 million
    - Equifax: (At least) $575 Million
    - Instagram: $403 million
    - TikTok: €345 million ($370 million)
    - T-Mobile: $350 million
    - Meta (Facebook): $277 million
    - WhatsApp: $255 million
    - Home Depot: ~$200 million
    - Capital One: $190 million
    - Uber: $148 million
    - Morgan Stanley: $120 million (total)
    - Google Ireland: $102 million

This does not include the cost of brand reputation

According to a recent study by DLA Piper, more than 130,000 personal data breaches were reported to European data protection authorities in 2021 alone – an average of 356 notifications per day, an 8% increase from the average of 331 notifications / day in 2020. As a logical consequence, total fines have increased almost sevenfold compared to the previous year, reaching the billion mark, according to the study.

The ‘Why’ and the Opportunities

The GDPR “domino” effect in the U.S. is here, and ongoing. As of Feb 23, 2024, current consumer privacy laws in the U.S.

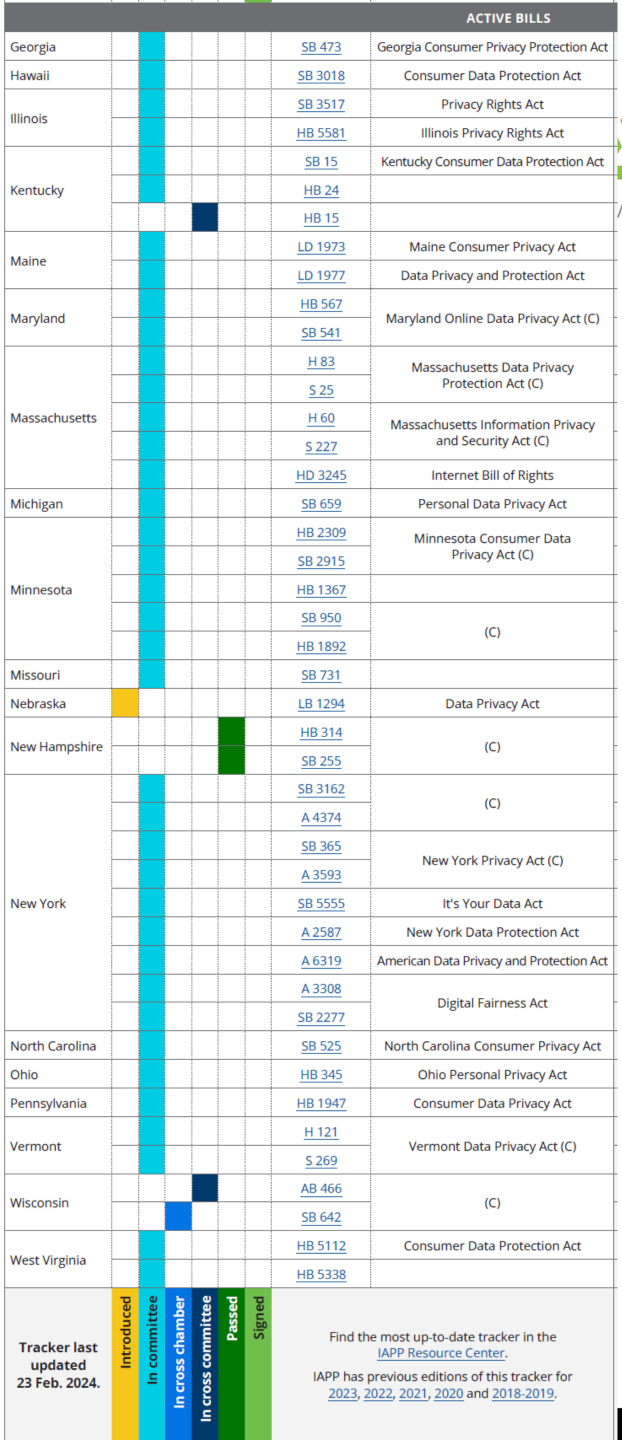


State	Legislative process	Statute/bill	Common name
			LAWS SIGNED (TO DATE)
California	🟩	CCPA	California Consumer Privacy Act (2018; effective 1 Jan. 2020)
	🟩	CPRA	California Privacy Rights Act (2020; fully operative 1 Jan. 2023)
Colorado	🟩	SB 190	Colorado Privacy Act (2021; effective 1 July 2023)
Connecticut	🟩	SB 6	Connecticut Data Privacy Act (2022; effective 1 July 2023)
Delaware	🟩	HB 154	Delaware Personal Data Privacy Act (2023; effective 1 Jan. 2025)
Indiana	🟩	SB 5	Indiana Consumer Data Protection Act (2023; effective 1 Jan. 2026)
Iowa	🟩	SF 262	Iowa Consumer Data Protection Act (2023; effective 1 Jan. 2025)
Montana	🟩	SB 384	Montana Consumer Data Privacy Act (2023; effective 1 Oct. 2024)
New Jersey	🟩	SB 332	(2024; effective 15 Jan. 2025)
Oregon	🟩	SB 619	Oregon Consumer Privacy Act (2023; effective 1 July 2024)
Tennessee	🟩	HB 1181	Tennessee Information Protection Act (2023; effective 1 July 2025)
Texas	🟩	HB 4	Texas Data Privacy and Security Act (2023; effective 1 July 2024)
Utah	🟩	SB 227	Utah Consumer Privacy Act (2022; effective 31 Dec. 2023)
Virginia	🟩	SB 1392	Virginia Consumer Data Protection Act (2021; effective 1 Jan. 2023)

The ‘Why’ and the Opportunities

The GDPR “domino” effect in the U.S. is here, and ongoing. As of Feb 23, 2024, active bills for consumer privacy:

Source: https://iapp.org.



ACTIVE BILLS

State	Introduced	In committee	In cross chamber	In cross committee	Passed	Signed	Bill	Title
Georgia		■					SB 473	Georgia Consumer Privacy Protection Act
Hawaii		■					SB 3018	Consumer Data Protection Act
Illinois		■					SB 3517	Privacy Rights Act
		■					HB 5581	Illinois Privacy Rights Act
Kentucky		■					SB 15	Kentucky Consumer Data Protection Act
		■					HB 24	
				■			HB 15	
Maine		■					LD 1973	Maine Consumer Privacy Act
		■					LD 1977	Data Privacy and Protection Act
Maryland		■					HB 567	Maryland Online Data Privacy Act (C)
		■					SB 541	
Massachusetts		■					H 83	Massachusetts Data Privacy Protection Act (C)
		■					S 25	
		■					H 60	Massachusetts Information Privacy and Security Act (C)
		■					S 227	
		■					HD 3245	Internet Bill of Rights
Michigan		■					SB 659	Personal Data Privacy Act
Minnesota		■					HB 2309	Minnesota Consumer Data Privacy Act (C)
		■					SB 2915	
		■					HB 1367	
		■					SB 950	(C)
		■					HB 1892	
Missouri		■					SB 731	
Nebraska	■						LB 1294	Data Privacy Act
New Hampshire					■		HB 314	(C)
					■		SB 255	
New York		■					SB 3162	(C)
		■					A 4374	
		■					SB 365	New York Privacy Act (C)
		■					A 3593	
		■					SB 5555	It's Your Data Act
		■					A 2587	New York Data Protection Act
		■					A 6319	American Data Privacy and Protection Act
		■					A 3308	Digital Fairness Act
		■					SB 2277	
North Carolina		■					SB 525	North Carolina Consumer Privacy Act
Ohio		■					HB 345	Ohio Personal Privacy Act
Pennsylvania		■					HB 1947	Consumer Data Privacy Act
Vermont		■					H 121	Vermont Data Privacy Act (C)
		■					S 269	
Wisconsin				■			AB 466	(C)
			■				SB 642	
West Virginia		■					HB 5112	Consumer Data Protection Act
		■					HB 5338	

Tracker last updated 23 Feb. 2024.

Find the most up-to-date tracker in the IAPP Resource Center.

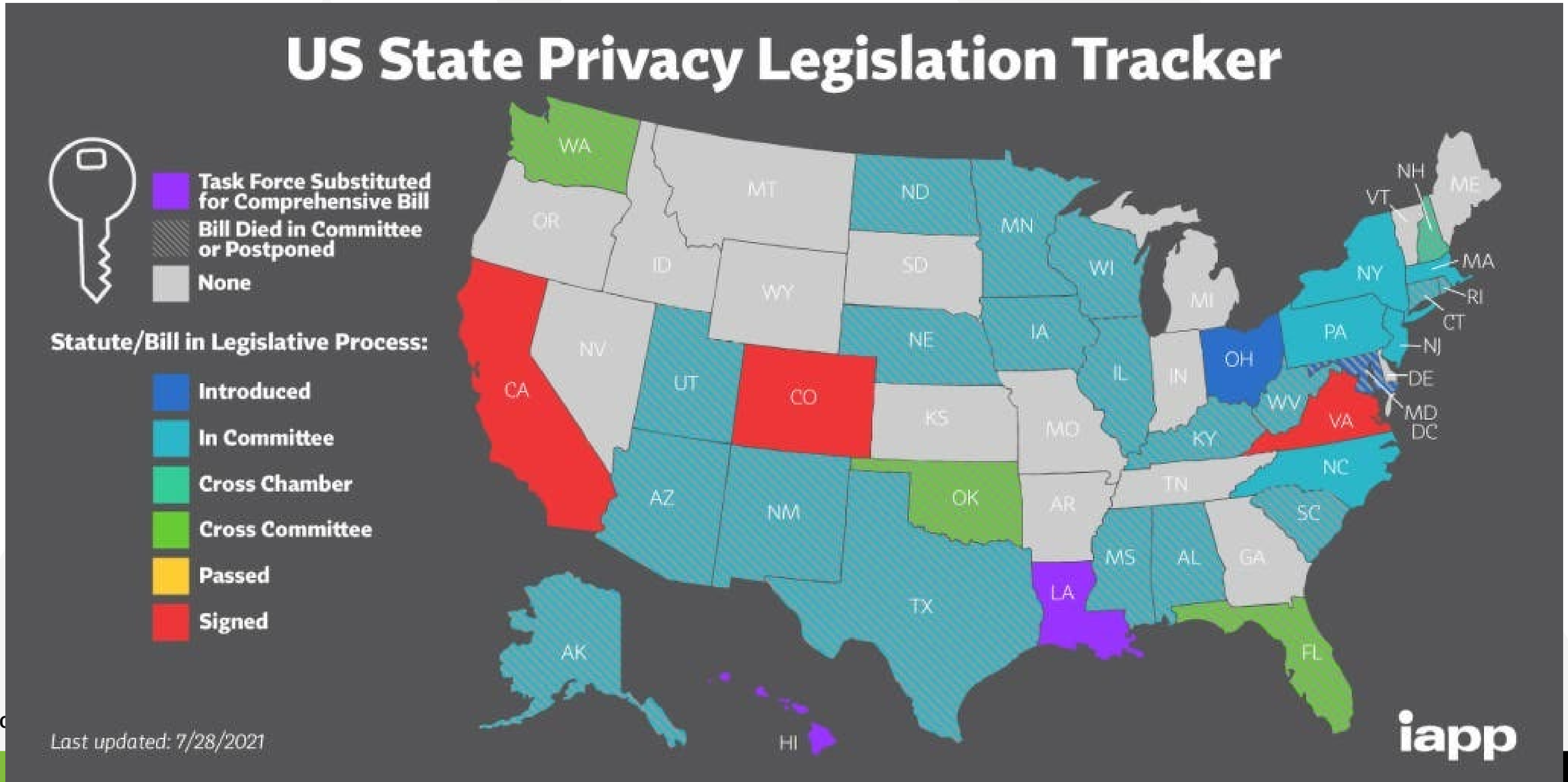
IAPP has previous editions of this tracker for 2023, 2022, 2021, 2020 and 2018-2019.

The ‘Why’ and the Opportunities

- IT is focused on delivery of functional, quality technical results
  - Always on the lookout for “gotchas” like regulations, laws, liability, capacity limits
- Marketing wants to create quality, compelling messaging that connects and drives opportunities for sales or direct purchase
  - “Know thy customer” is essential to avoid wasted effort
- Like two ships that crash in the night
  - IT and marketing don’t automatically perceive common ground
  - When their requirements suddenly conflict, resolution is unclear
- Unique opportunity for communication and partnership
  - Establishing a clear mutual understanding of needs and boundaries
  - Designating relationship connectors
  - Brainstorming emergent opportunities from available data and functionality
  - Both of us work within the “abstract,” not easily understood.

Get Ready, You’re About to Lose Sleep!

- It took a few years for punitive damages to sink in in Europe, about 3 years for Amazon fine of 2021. In the U.S., fines are undoubtedly coming.
- You likely understand security and compliance well, but what about privacy (PII) and compliance?



What can you do to help you sleep better?

- Organizations are obliged to protect their user's
  data and understand the data they need to safeguard.
- **Personal data**, in the context of GDPR, covers a much wider range of information than **personally identifiable information (PII)**, commonly used in North America.
- In other words, while all PII is considered personal data, not all personal data is PII.
- **Footprints & Forensics**
  - Few people today are fully aware of how many traces of personal information they leave every day
    in this increasingly digital and interconnected world
  - Those identifying details are Personally Identifiable Information (PII), which is the key element in
    privacy policies, data protection, government regulations and a variety of tech crimes. The more PII we produce, the more complex it becomes keeping it safe.

What is ‘PII’ ultimately?

USA: the Guide to Protecting the Confidentiality of Personally Identifiable Information (PII). published by the National Institute of Standards and Technology (NIST), provides the most widely used definition of PII:

“PII is any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual‘s identity, such as name, social security number, date and place of birth, mother‘s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.”

1 Sentence, 62 words + 11 commas or simply “PII is any type of information that can identify an individual”

Despite the wide variety and sensitivity of such information, there is not a single, global definition of Personally Identifiable Information or what types of information it encompasses.

As a result, definitions of PII can differ among organizations and across borders:

- Sensitive PII
- Non-Sensitive PII
- Non-Personally Identifiable Information
- Linked/Sensitive PII
- Linkable or Non-Sensitive PII

So, Now You Must Manage Data Security and PII!

Examples of linked/sensitive PII:

- first and last name
- home address
- email address
- telephone number

What is non-sensitive PII?

Referred to as linkable data, because it requires more data elements to be linked together to establish an individual's identity. Whereas sensitive PII can reveal identity on its own or with very limited combined information sources.

Examples of linkable or non-sensitive PII:

- first or last name (if it's common)
- mother's maiden name
- partial address, like a country or zip code
- age range, e.g. 35-44
- date of birth
- gender
- employer

Managing Both Data Security and PII

What is non-Personally Identifiable Information?

Non-Personally Identifiable Information is data about a person, or data resulting from their activities, that on its own cannot be used to identify someone. This could be because the information is already anonymous and part of a larger data set, or because it has been anonymized.

Examples of non-Personally Identifiable Information:

- IP addresses that have been fully or partially masked
- Aggregated statistics from the user base for a product or service
- Data that has been anonymized by encryption, removal of identifying information, or other technique

Managing Both Data Security and PII

What is a PII violation?

A company, for example, must protect customer data to the standards set by their corporate privacy and security policies. But they must also meet the standards of local state and federal governments and trading partners to avoid PII violations.

Types of PII violations

PII violations can include data breaches where millions of detailed records are stolen.
They can also include lower-level breaches, like companies not adequately limiting access to and sharing of data between internal departments, or with contractors. Or organizations may not adequately anonymize data before providing it to customers, partners, or researchers.

Footprints & Forensics

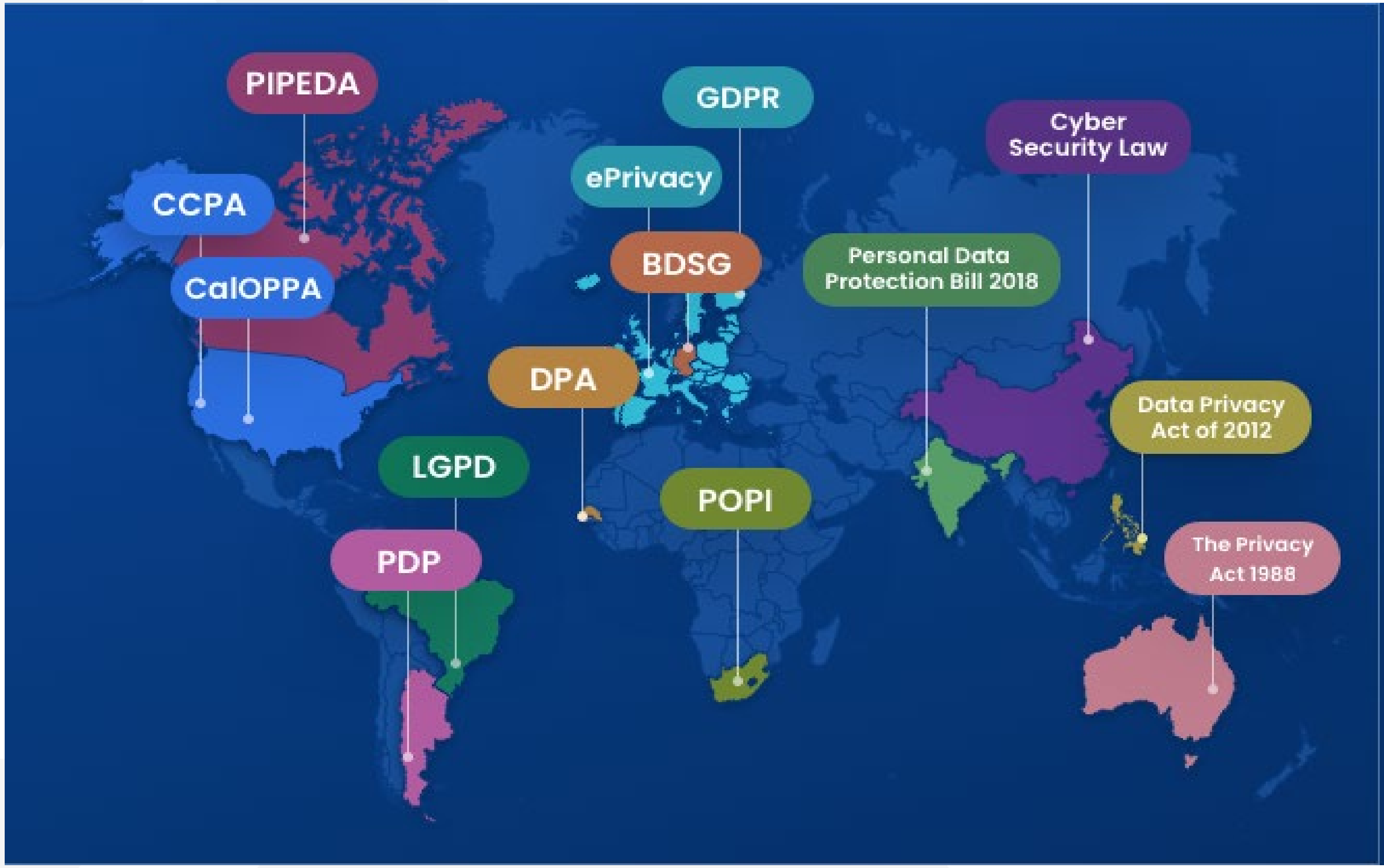
Every contact leaves a trace, and in an increasingly digital and interconnected world, there are more contacts among individuals and organizations than ever before. Few people today are fully aware of how many traces of personal information they leave every day.

Managing Both Data Security and PII

Privacy Laws per Country

GDPR, CCPA, HIPAA, SHIELD ……

All data privacy laws have two things in common: data protection and breach notification requirements.



Managing Both Data Security and PII

Organizations and Persons Responsible

The primary role of the data protection officer (DPO) is to ensure that the organization processes the personal data of its staff, customers, providers or any other individuals (also referred to as data subjects) in compliance with the applicable data protection rules.

Tasks of the DPO

The DPO has to ensure that the data protection rules are respected in cooperation with the data protection authority (DPA)

The ideal DPO

The DPO should have expert knowledge of data protection and a good understanding of the way the organization operates.

The DPO should only report to top management.

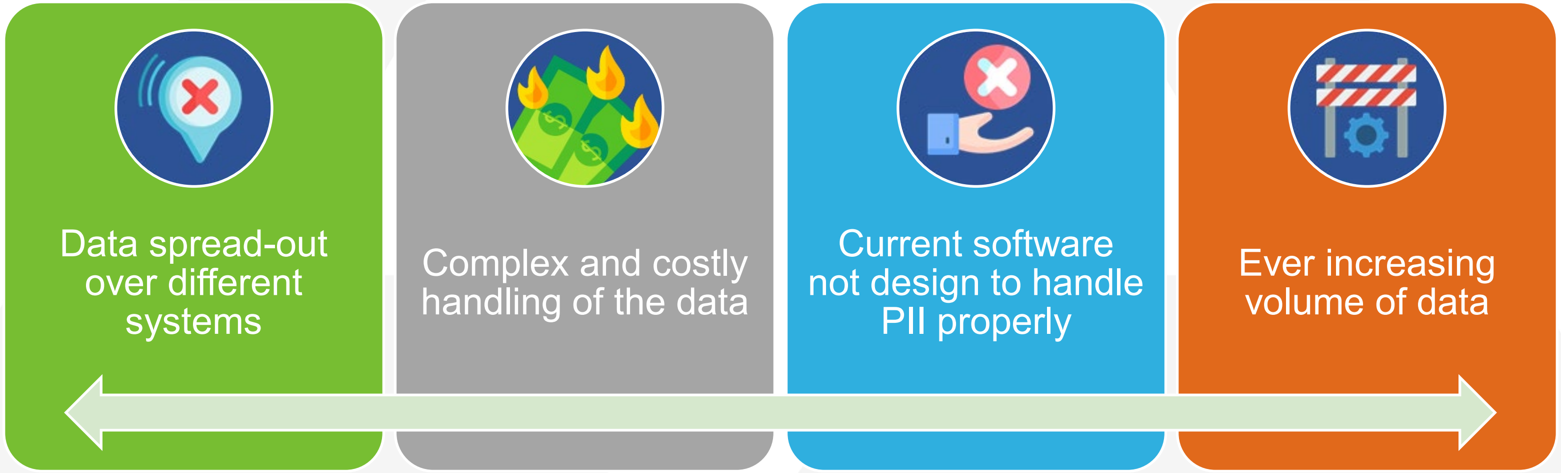
Who is the DPO at your company?

Managing Both Data Security and PII

Where is PII stored?

- LUW- and Mainframe servers & databases
- Difficult to localize
- Difficult to adapt business & compliance rules

Maintaining Data Privacy and Compliance is not trivial and is definitely not a one-time job !



Data spread-out over different systems

Complex and costly handling of the data

Current software not design to handle PII properly

Ever increasing volume of data

Data Retention and Deletion

The CCPA (previous law) had no requirement. The CPRA does stipulate retention requirements. The CPRA is essentially an amendment to the CCPA, and adds as key component, retention.

Again, the GDPR's influence

Your To-Do: Classify data based on business needs

Data Retention Policy

- One of the fundamental principles of the GDPR is that personal data should not be retained for longer than necessary.

How long can (may) personal data be stored?

- This depends on various factors, including the type of data, the purpose for which it was collected, and the legal and regulatory requirements that apply.
- In some cases, personal data may only need to be stored for a short period, such as for the duration of a transaction. In other cases, personal data may need to be stored for extended periods, such as for historical research purposes.

We Are Here To Help You Sleep!

What can you do to help you sleep better?

- You can’t remediate or take action on what you can’t see
  - Up-to-the-second visibility is key
- Understand that the main principles of GDPR also reside in states’ legislation
  - Personal Data (GDPR) and Personally Identifiable Information (PII) are defined explicitly as a protection measure for citizens. *GDPR’s origins date back to the Nazis identifying Jews for the oppression they would soon give.*
  - Both allow some type of control by citizens of their personal information, mainly removal or objection to use of their personal information.
    - The caveat is you have to know where all the data is in you are required to remove them. Visibility is key.
  - Both have exceptions by organizations to deny removal (contracts, police investigations, other similar).
  - Both define who is the “controller” – business (CCPA) vs. DPO (GDPR)
  - Upon request, you must give individuals full visibility of the data your org holds on them.
    - With CCPA, you must give up the data and sources of the data
  - You must give data subjects at least 2 methods to access the information you have on them.
  - BOTH HAVE PENALTIES! And, both have a means to seek cause of action for damages that is provided by the state.

See Future of Privacy Forum for more info – https://fpf.org

What can you do to help you sleep better?

- There is software that can help you manage CCPA, GDPR, and other PII management needs.
- The Privacy Compliance and Data Security Compliance markets are converging. As is the case there is not 1 solution that can do both.
- Because Privacy Policy is managed by Ops and Legal business titles and InfoSec is generally handled by IT titles YOU MUST START TALKING TO YOUR BUSINESS/OPS PEERS:
  - CMO – has access to all the prospecting data, tons of PII and IP
  - CEO – tells CMOs what to do without understanding what CMOs do
  - COO – Helps CEOs tell CMOs what to do without understanding what CMOs do
  - CLO – Does what the CEO and COO tell them and doesn't know what anyone does
  - CHRO – *This is a very good place to start communicating as the number one threat in your org is human error, human negligence, and/or bad human actors with access to your network. The CHRO can help educate at employee onboarding.*

What You IT Folks Do About This?

- Install Java (i.e. have coffee)
- Identify common sources of mandate, demand, difficulty
- Find places of conflict, trace roots to business reasons and values
- Meta-silo communication and relationship

How Collaboration Should Work Across IT, Marketing, HR, and the Core Business

- **IT:** Stewardship of the data *for the business*
- **Marketing:** Using the data *to generate business*
- **HR:** That data had better not be used for monkey business
- **Core business:** That data is a key aspect of our *business success*
- **Compliance:** Rules, regulations, laws: personally identifiable information

These things fill silos. Get out of your SILO!

So, What Does This All Mean?

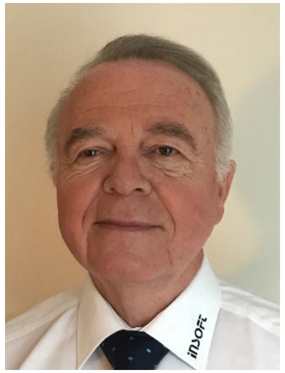
1. Lack of communication creates unknowns; unknowns are devastating for breach response
   - Communicate up and down the chain of command.
     - Data breach is mostly enabled by human error from resources being overtaxed and over-mandated.
2. Silos of workflows and information is evidence of lack of communication.
   - When breach forensics starts it's less effective when you have to flip the switch and start communicating
3. Comms about cyberthreat start with CHROs and employee onboarding!
4. Breaches are career killers and impact the bottom line:
   - *"In 2023, the average cost of a data breach globally reached an all-time high of $4.45 million. This figure represents a 2.3% increase from the previous year and a 15.3% rise from 2020."**

*CSO Online magazine July 31, 2023

INFOTEL GDPR COMPLIANCE USE CASE

Visibility Articulated

Q&A Forum



Colin Oakhill | LinkedIn
InSoft Software GmbH
Düsseldorf, Germany
co@insoft-software.de

Tony Perri | LinkedIn
Perri Marketing, Inc.
Chattanooga, TN
(423) 212-3127, ext. 1
tony@perrimarketing.com

THANK YOU!

Question & Answer Session:

Your feedback is important!

Submit a session evaluation for each session you attend at www.share.org/evaluation