

Privacy Law Compliance

June 4, 2024



1



Cameron G. Shilling
Chair, Cybersecurity and Privacy
McLane Middleton, P.A.
Email: cameron.shilling@mclane.com
Direct: 603-628-1351 Cell: 603-289-6806

Cam Shilling founded McLane Middleton's Cybersecurity and Privacy Group in 2009. His expertise includes managing information privacy and security risk assessments under domestic and international laws and regulations, preparing and implementing written policies, delivering workforce trainings, addressing day-to-day cybersecurity and privacy issues, investigating and remediating incidents and breaches, and defending against governmental audits and consumer and class action lawsuits.



2



*Danielle B. Lemack
Assistant General Counsel and V.P.
HP Hood LLC, Lynnfield, MA
Email: danielle.lemack@hphood.com*

Danielle is responsible at Hood for counseling business teams on a variety of issues, including privacy, information security, advertising, food packaging claims and regulatory compliance, licensing, contract negotiation, and litigation strategy. In addition to her legal work, she oversees the Product Regulatory Affairs team. Prior to joining Hood, Danielle was a partner at an intellectual property law firm in Chicago.



3

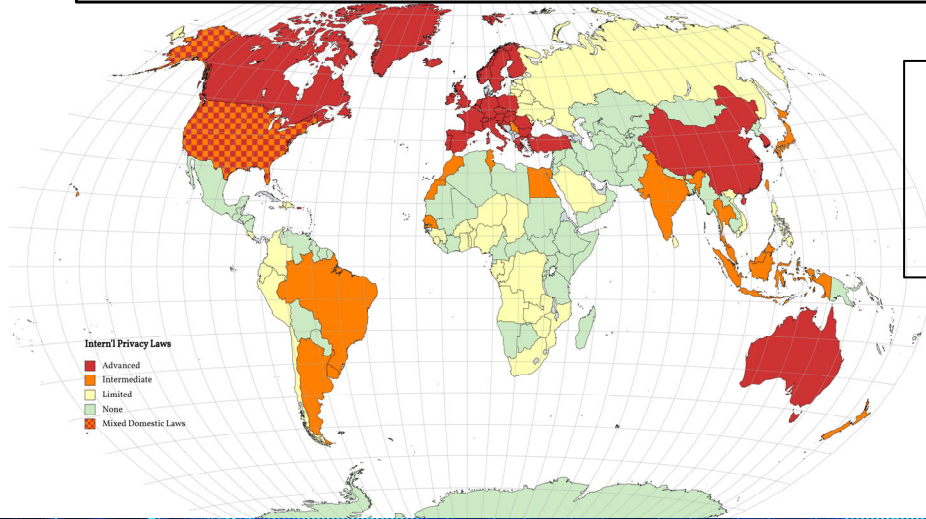
Outline of Presentation

- 1. Regulatory Landscape**
- 2. Champions of the Process**
- 3. Scope and Components of Laws**
- 4. Compliance Process**



4

Regulatory Landscape

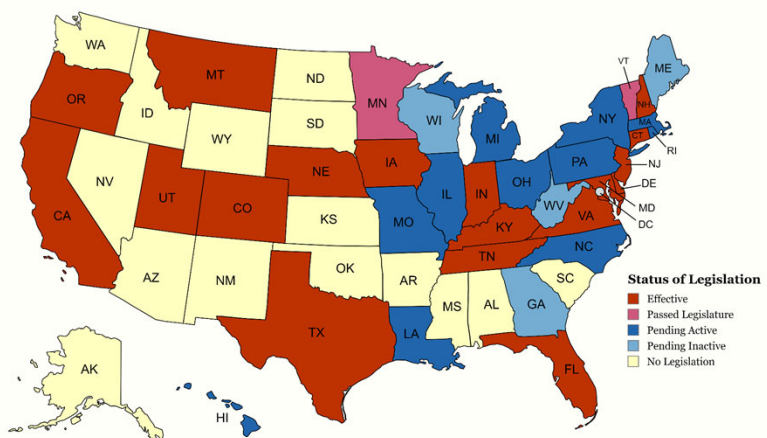


**Global
Privacy Law
Expansion**

5

Regulatory Landscape

**Privacy Laws
Spread Across
the Country**



6

Regulatory Landscape

Intra-Territorial Jurisdiction

- ✓ Permanent or temporary office or other facility
- ✓ Consistent travel by employees for business
- ✓ Employing resident w/processing pertinent to duties

Extra-Territorial Jurisdiction

- ✓ Consistent remote interactions with customers or vendors
- ✓ Consistent advertising to capitalize on business opportunities
- ✓ Consistent billing and payment interactions with customers or vendors



7

Regulatory Landscape

**Global and
National
Regulatory
Network**



8

Champions of the Process

CEO, COO, or Other C-Level Officer(s)

- Gravitas and institutional commitment
- Budgetary, operational, and cultural authority

In-House and Outside Counsel

- In-House: Project management and task completion
- Outside: Leadership ↔ Assistance ↔ Design ↔ Input

Lead Information Technology Officer(s) and Records Managers

- IT: Technological authority, knowledge, and expertise
- Records: File management authority, knowledge, and expertise

Departmental Business Manager(s)

- Awareness of vast majority of business operations
- Relationships with majority and most influential personnel



9

Scope and Components of Privacy Law

1. Personal information broadly defined
2. Differentiates controllers and processors
3. Thresholds: NH is 35,000/10,000 residents
4. Exclusions for certain businesses and info.
 - Privacy laws: HIPAA; GLBA; FERPA, FTCA ...
 - Employment, non-profits, specific others ...



10

Scope and Components of Privacy Law

1. **Notice:** policy delivered directly at initial collection
2. **Consent:** sensitive PI, sale, targeted ad/profiling
Race Religion Citizenship Immigration Ethnic Orig.
Children Politics Sex Life Sexual Orien. Health/Med.
SSN Gov. ID Financial Biometrics Geolocation
3. **Rights:** confirm, correct, obtain, opt-out, and delete
4. **Security:** tech/physical/admin measures, and DPIA
5. **Enforce:** AG or complaint to AG, but no private suit

11

Compliance Process

1. **Conduct assessment interviews**
2. **Implement policy and notice/consent**
3. **Create privacy rights request response**
4. **Prepare data privacy impact assessment**
5. **Construct management structure, internal policy, and workforce training**

12

Assessment Interviews - Purposes

1. Points of entry of PI for notice and consent
2. Types of PI/sensitive PI for policy and DPIA
3. Types of processing activities for privacy policy
4. Applications and SaaS used for notice and consent
5. Methods of retention for privacy rights fulfillment
6. Disclosures to third-parties for diligence and DPAs
7. Safeguards for cybersecurity compliance and DPIA

13

Assessment Interviews - Scope

Retail and Manufacturing

1. IT, website and CRM
2. Customer apps and portals
3. Sales, quoting, ordering
4. Product devo and R&D
5. Fulfillment and ERP
6. Accounting and finance
7. Payment and POS
8. Service and warranty

Services and Professional

1. IT, website and CRM
2. Client apps and portals
3. Engagement and SOW
4. Service departments
5. Accounting and finance
6. Administration
7. Partners and affiliates
8. Client disengagement

14

Components of Privacy Policy

1. PI processed
2. Sensitive PI processed
3. Processing activities
4. Legal bases to process
5. Types of processors/subs
6. Individual privacy rights
7. Rights request mechanism
8. Response, timing, appeal
9. Identify privacy officer
10. Selling, ads and profiling

15

Notice and Consent

1. Requirements and Methods for Notice and Consent
 - Notice: Inform about privacy policy and provide link
 - Consent: Knowing and affirmative act of acceptance
Logged and retained in key records, apps and SaaS
2. Timing to Provide Notice and Obtain Consent
 - First collection of personal information
 - Collection of meaningful additional or different information
 - Change in law or in business's policy or processing activities

16

Privacy Rights Request and Response

1. Webpage and other mechanism to exercise privacy rights
2. Procedure to follow to address privacy rights requests
 - Assess sufficiency of request
 - Authenticate identity and authority
 - Obtain necessary additional info
 - Confirm receipt and set expectations
 - Identify all personal information
 - Assess potential legal restrictions
 - Inform if additional time is needed
 - Fulfill request in business systems
 - Ensure compliance by third parties
 - Inform individual of outcome
 - Inform about appeal rights
 - Maintain log of activities



17

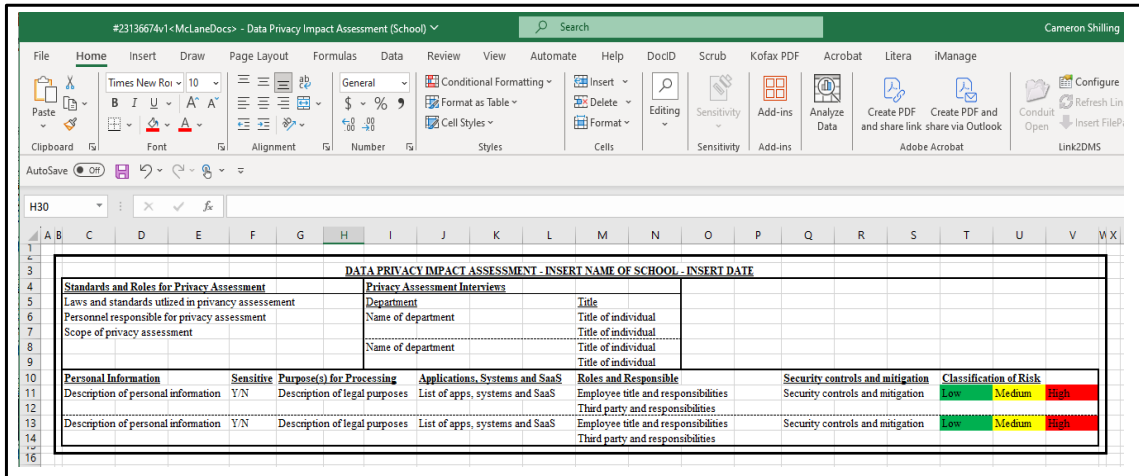
Data Privacy Impact Assessment

1. Identify laws/standard
2. Summarize assessment
3. Identify PI/sensitive PI
4. List processing activities
5. Map PI in apps and SaaS
6. Identify responsibilities
7. List processors/subs
8. Identify security risks
9. Describe mitigations
10. Classify levels of risk



18

Data Privacy Impact Assessment



DATA PRIVACY IMPACT ASSESSMENT - INSERT NAME OF SCHOOL - INSERT DATE						
Standards and Roles for Privacy Assessment			Privacy Assessment Interviews			
Laws and standards utilized in privacy assessment			Department	Title		
Personnel responsible for privacy assessment			Name of department	Title of individual		
Scope of privacy assessment			Name of department	Title of individual		
Personal Information			Sensitive	Purpose(s) for Processing	Applications, Systems and SaaS	Roles and Responsible
Description of personal information	Y/N	Description of legal purposes	List of apps, systems and SaaS	Employee title and responsibilities	Third party and responsibilities	Security controls and mitigation
Description of personal information	Y/N	Description of legal purposes	List of apps, systems and SaaS	Employee title and responsibilities	Third party and responsibilities	Security controls and mitigation
						Classification of Risk
						Low Medium High
						Low Medium High

19

Management, Internal Policy and Training

1. Management Structure – Privacy Officers

- Lead Information Technology Officer(s)
- In House Counsel and Records Managers
- CEO, COO or Other C-Level Officer

2. Internal Cybersecurity and Privacy Policy

- Complies with both cybersecurity and privacy laws
- Enumerates privacy rights for personal information

3. Workforce Training, Testing and Re-Training

- Train at time of policy adoption and periodically thereafter
- Routine testing of employees, and re-training as appropriate

20



Cameron G. Shilling
Chair, Cybersecurity and Privacy
McLane Middleton, P.A.
Email: cameron.shilling@mclane.com
Direct: 603-628-1351 Cell: 603-289-6806



Danielle B. Lemack
Assistant General Counsel and V.P.
HP Hood LLC, Lynnfield, MA
Email: danielle.lemack@hphood.com



21

Privacy Law Compliance

June 4, 2024



22