Let’s Get Digital

Privacy & Data Security Best Practices in the Workplace

Jeff Duncan Brecht
Shareholder

LANE POWELL

Emily M. Maass
Attorney

11.4 .2019

Bureau of Labor & Industries: BOLI's 35th Annual Employment Law Conference

Disclaimer

This presentation reflects the views of its author, which are not necessarily the views of BOLI or Lane Powell PC.

It is intended to provide general information only.

It is not intended to provide any legal opinions or advice applicable to any particular situation, and does not create an attorney-client relationship with any attendee or reader.

If you would like more information regarding whether we may assist you in any particular matter, please contact one of our attorneys. Use care not to provide us with any confidential information until we have notified you in writing that there are no conflicts of interest and that we have agreed to represent you on the specific matter that is the subject of your inquiry.

PRIVACY, CONFIDENTIALITY, and DATA BREACHES

WHAT'S AT STAKE FOR EMPLOYERS?

Jeff Duncan Brecht
Shareholder

Concern No. 1
Public Relations Problems

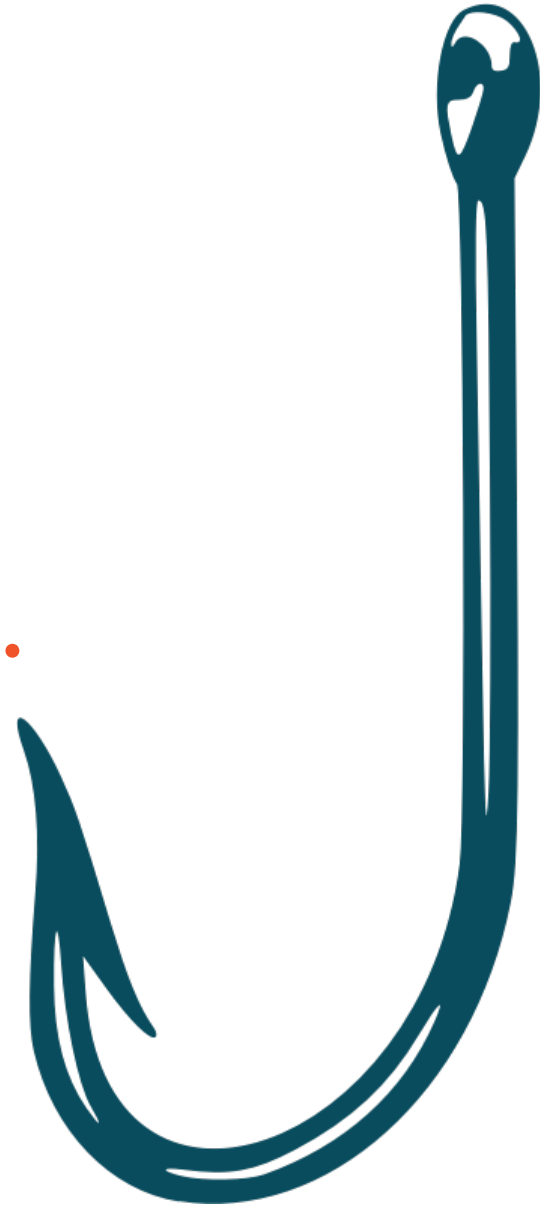
- Most states, including Oregon, require businesses to notify their "customers" as soon as possible if there has been a data security breach. (*See* ORS 646A.600 - 646A.628.)
- Depending on the scope of the breach, employers may also be required to notify the Oregon Attorney General.

Public Relations Concern
Real Life Adventure

- 08.24.2019 – Forbes : “Instagram Security Warning: Millions At Risk From ‘Believable’ New Phishing Attack.”

  - “..this is a phishing campaign with a devious twist….We don't like to admit it," the research team reports, "but the crooks thought this one through."

Speaking of "phishing attacks"... what are they?



Concern No. 2
Lawsuits!

Real Life Adventure: Lawsuits Against Employers By Their Own Customers

- 10.03.2018 (Oregon) (alleged data breach):

Cassadra Nelson, individually and on behalf of other customers (Plaintiff)

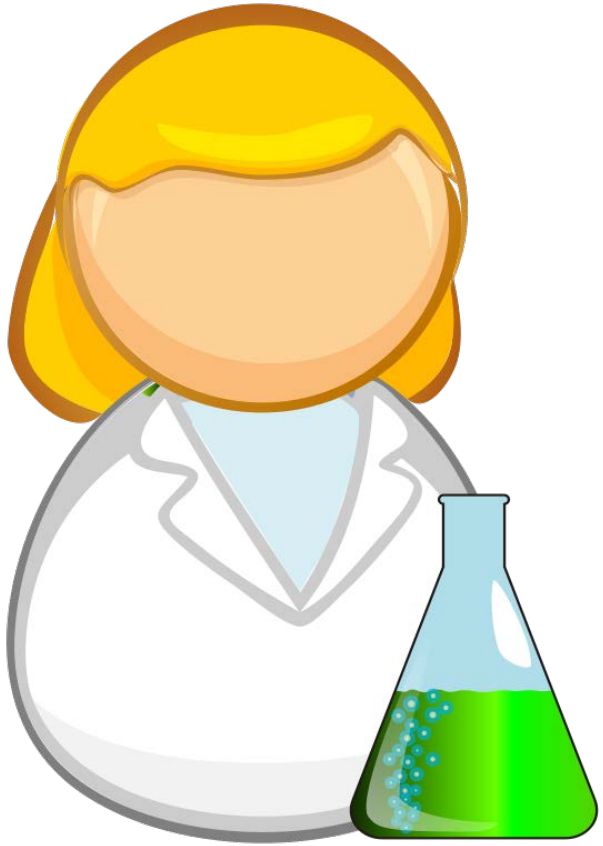
vs.

Burgerville LLC (Defendant)

Real Life Adventure: Lawsuits Against Businesses By Their Own Employees

- Nov. 2018 (PA Sup. Court) Employee class action re data breach. Found businesses owe their employees a duty to exercise reasonable care when collecting and storing personal and financial information .

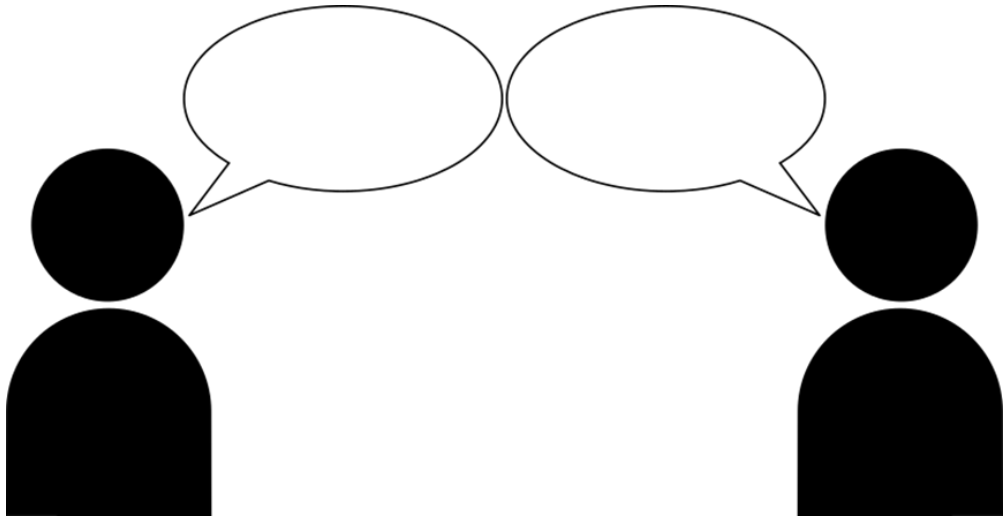
Dittman v. UPMC



Concern No. 3
Medical Information & Records in the Workplace

Medical Information and Records in the Company

(medical leave, worker's comp, disability accommodations..)



Real Life Adventure
Possible HIPAA Violations

- For HIPAA -covered employers, an employee -caused data breach could also be a HIPAA breach
- If so, employer could be liable for sanctions and also required to provide notifications of the breach
- Depending on the scope of the breach, employer might even be required to notify the media

Concern No. 4
Employer Business Disruption

Let's Get Real…

How Much Time Will It Take to Deal with a Privacy/Data Misstep or Breach?

So…

Employer's Four (Preliminary) Steps

1. Assess the employee -related privacy and data security risks.
2. Develop/revise employee privacy and data security policies that address and mitigate related risks.
3. Educate and train employees on compliance with the privacy and data security policies.
4. Implement and enforce employee -related privacy and data security policies.

Step One: Assess Employee -Related Privacy and Data Security Risks

The information garnered from this employee -related privacy and data security risk assessment process is essential to create and implement workplace privacy and data security policies, practices, and training that most effectively fit and protect your workplace.

What Questions Should Employers Ask?

- Employers should modify their assessment to best fit their particular circumstances
- In general, employers should include at least the following queries in their employee-related privacy and data security risk assessment:

- What policies are in place to make sure that only employees who need to have access to private data have access to that data?
- Do employees have nonpublic workspaces where they may privately discuss customer / business matters?
- What password policies and practices must employees comply with?

- Does employer require employees to utilize encryption technology to protect private data?
- Are employees required to promptly remove and secure materials from printers and fax machines?
- Do employees log out of workstation computers, tablets, and laptops before they step away?
- How quickly (if at all) do employee workstation computers, tablets, and laptops "auto lock" when those devices are inactive?

- Do employees transport private, work-related information in their vehicles?
- Do employees use laptops and other devices that contain private, work-related information at their homes, coffee shops, or elsewhere offsite?
- Is private, work-related information visible to customers, visitors or the public at employee workstations?

- Do employees verify e-mail addresses and fax numbers before transmitting private information?

- How (if at all) do employees report violations of Company's privacy and data security policies?

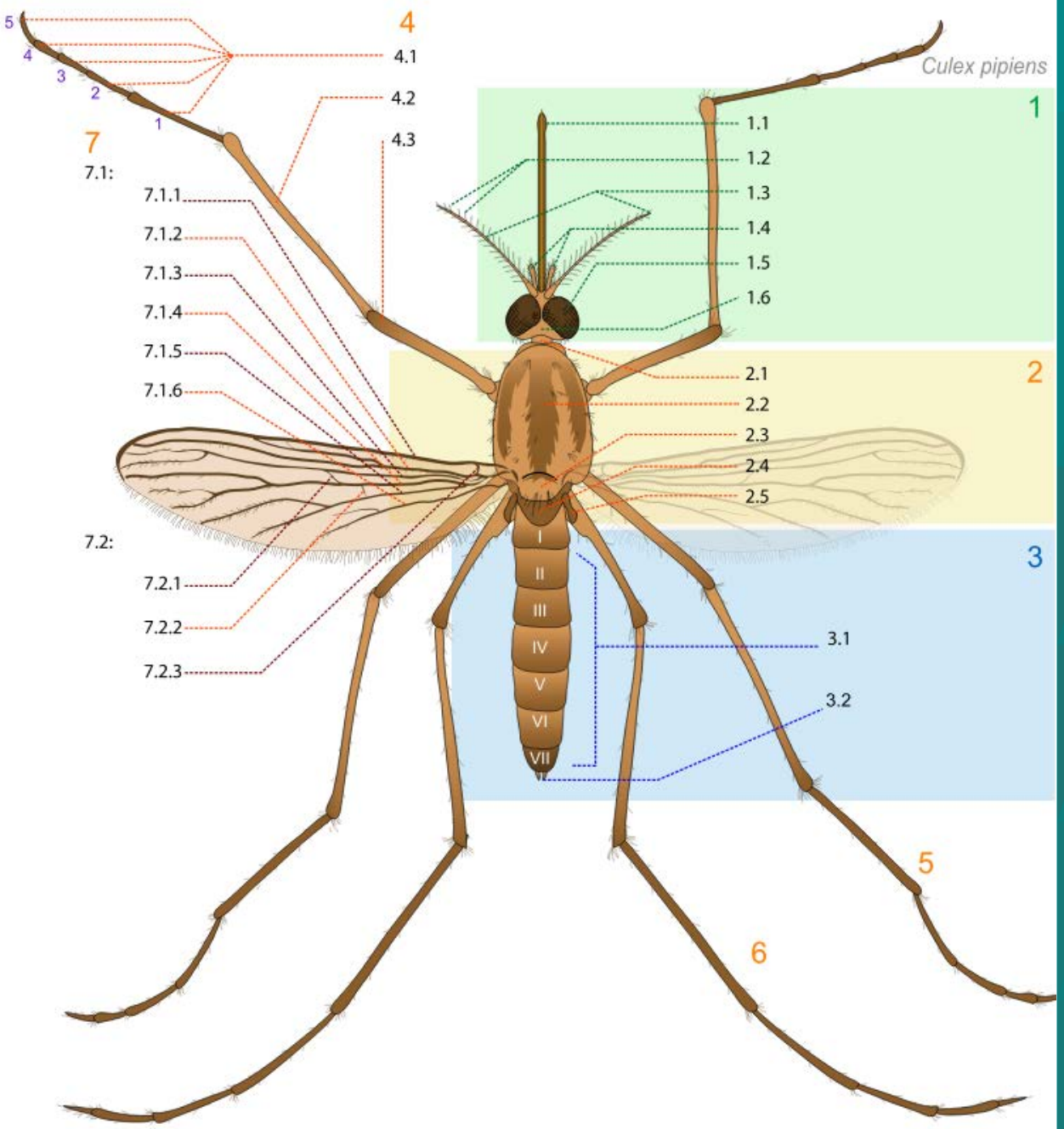
- Are employees aware that their coworkers also have privacy rights and that they should not access each other's information?

- Do employees know whom to approach with their privacy and data security questions and concerns?

- Are employees trained on workplace privacy and data security? If so, how?

Real Life Adventure – Ransomware

If employer's computer systems are infected with a ransomware virus, then employer may not be able to access data necessary to conduct business.



Anatomy of a Ransomware Attack

Who performs the employee -related privacy and data security risk assessment?

LANE POWELL

A team leader: An individual with primary responsibility for coordinating and moving the assessment along

Stakeholders: Employees who actually work with private information at your workplace (this should include HR representatives and other employees, as appropriate)

Someone to document the process: Someone responsible for accurately documenting the good faith efforts employer undertakes to assess employment -related privacy and data security risks —and conclusions/actions

Appropriate tech experts: Someone knowledgeable about the data systems employer/employees currently use, current security measures, and related privacy and data security vulnerabilities

Assessment – Cost vs. Benefit?

- *This employee -focused risk assessment seems like a ginormous investment of time and money:*
  - Investing the necessary resources to assess employee -related privacy and data security risks and to develop policies and practices to mitigate those risks is an investment prudent employers will undertake.
  - It may prevent a breach.
  - Moreover , in the event of a privacy breach, liability might be higher if employer did not take reasonable steps to discover breach risks and mitigate against them.
  - An ounce of prevention…

Step Two: Develop Employee -Related Privacy and Data Security Policies & Practices

- There is no one -size-fits-all group of employee -related privacy and data security policies and practices.

- However , based on the information gleaned from the risk assessment, most employers will want to develop (or revise) employee -related policies that address at least the following employee -focused components:

Every employee is responsible for privacy and data security compliance.

- Employer's policies should emphasize that every employee is expected to be a team player dedicated to respecting and protecting employer, customer and coworker privacy and data security.

If you see something, say something.

- Make sure policies state that employees must immediately report suspected privacy breaches. Your policy should identify who needs to be notified and how.

Retaliation prohibited.

- Policies should emphasize that (1) employees who make good faith reports of suspected privacy and data security policy violations are protected from retaliation and (2) employees who violate the "no retaliation" policy are subject to discipline up to and including termination. The policy should also provide options for employees to report retaliation.

A "need -to -know" basis:

- Employer's policies should help make sure that only employees who need to have access to private data have access to that data.

Workstations:

- Policies should help make sure that private information cannot be viewed by customers or the public.

Employer computers and devices:

- Policies should ensure that employees accessing private information maintain the privacy of that information (i.e., use of passwords, logging off when stepping away from computers, maintaining physical control of employment -use devices).

Use of copiers and fax machines:

- Policy should include employee protocols to make sure privacy is maintained (i.e., documents with private/sensitive information are not left unattended on copiers, etc.).

Key Tip
Manage Employee Privacy Expectations

- Employees who use employer's technology for personal e-mails and texts may assume employer has no right to monitor that personal use. But….

- …if employer has a written policy that expressly informs employees that employer reserves the right to monitor and review employees' personal use of employer's technology, and that employees should have no expectation of privacy regarding such personal use, such a policy may overcome an employee's objection to such review and monitoring.

Another Key Tip
Have a Social Media Policy

Social Media Policy should inform employees how their use of social media may impact such things as:

- Company's trade secrets;
- Confidential customer information; and
- Employee rights to be free from harassment and retaliation.

BUT..make sure social media policy does not violate employee rights—such as the right to freely engage in "concerted activity" related to the terms and conditions of employment and/or whistleblowing rights.

The following employee social media policies are probably appropriate:

Encourage employees to be vigilant online to avoid being tricked into disclosing confidential information.

Encourage employees to notify management of Company safety or other concerns.

Remind employees of the manner in which they may report Company concerns to management.

Remind employees that they are prohibited from bullying, discriminating and retaliating against their coworkers.

Prohibit employees from representing in social media that the employees speak for/on behalf of the Company.

Word of Caution
Social Media and Hiring Decisions

At first blush, it might seem that those persons who make hiring decisions for employers should do some “Googling” to determine if job applicants’ social media postings contain information relevant to application.

Some job applicants post things on social media that could reflect badly on their ability to perform their jobs.

But some job applicants also make information available online that employers should not consider as part of the hiring process.

LANE POWELL

It is not unusual for job applicants' social media postings to contain the following types of information:

- ethnicity and national origin
- workplace injuries and information about worker's compensation claims
- workplace complaints
- union affiliation and organizing activities
- religious affiliation and practices
- family status
- gender identity
- sexual orientation

The list of such information goes on and on.

Best Practices
Hiring in the Age of Social Media

- Human resources professionals should be better able to focus solely on nondiscriminatory information .
- Be consistent . If employer decides to review job applicants' public social media postings, make that the practice for all jobs (or at least, for all the same positions).
- Print it . If employer decides to take adverse action based on an applicant's (or employee's) social media posting, print and maintain a copy of that posting. That way, if the posting is later deleted, employer will have a copy available to show the legitimate, lawful, nondiscriminatory basis of its decision.

Step Three : Train Your Employees to Comply With Privacy and Data Security Policies & Practices

Even the most clearly written and comprehensive policies on employee -related privacy and data may not be effective unless employees are not only required to review those policies but are also given adequate and thorough training.

Make it part of new -hire orientation.

- New employees can be overwhelmed by the sheer volume of information that comes with a new job. Nonetheless, be sure to include privacy and data security policies and practices as part of new hire orientation.

Make comprehensive training an annual event.

- Because of the frequent changes in technology and privacy laws, it can be hard to keep up. Employers should provide comprehensive refresher training on privacy and data security policies and practices at least annually.

Provide mini -updates.

- Include 5 - to 10-minute updates on a specific area of your privacy and data security policies at weekly, bi -weekly, and/or monthly staff meetings. This helps employees remember how important privacy and data security is to employer.

Document each training session: It cannot be overemphasized how important it is for employers to maintain timely, complete, and accurate records of the privacy and data security training provided to employees.

- Have employees sign and initial policies —and maintain a signed/initialed copy.
- When employer provides training to employees on these policies, make sure every employee who attends that training signs and dates a document to evidence their participation in such training.
- If employee is disciplined for violating employer's privacy and data security policies, this documentation can be evidence that the adverse employment decision was not for a discriminatory or retaliatory reason.

Low -Tech Takeaway

LANE POWELL

Sticky Note

On workstation computer monitor, place a sticky note that states: *Stop and Think Before You Click That Link .*

It's a persistent reminder to help avoid a ransomware or other malicious software attack by taking a wary look at the e-mails received, especially where they have attachments or include internet links.

Step Four: Implement and Enforce Employee Privacy and Data Security Policies & Practices

- Employee -related privacy and data security policies will only be effective if they are implemented and enforced.

- Make privacy and data security a core part of your workplace culture.

Critical Managerial/Supervisory Role in Implementation

Train (and retrain) supervisors to lead by example when it comes to privacy and data security policy compliance.

- Employees who feel singled out for discipline are more likely to claim the discipline was discriminatory or retaliatory.

Two Additional Steps

Step 5: Breach Response Plan

Develop policies and procedures, and conduct training on what to do in the event of a data breach.

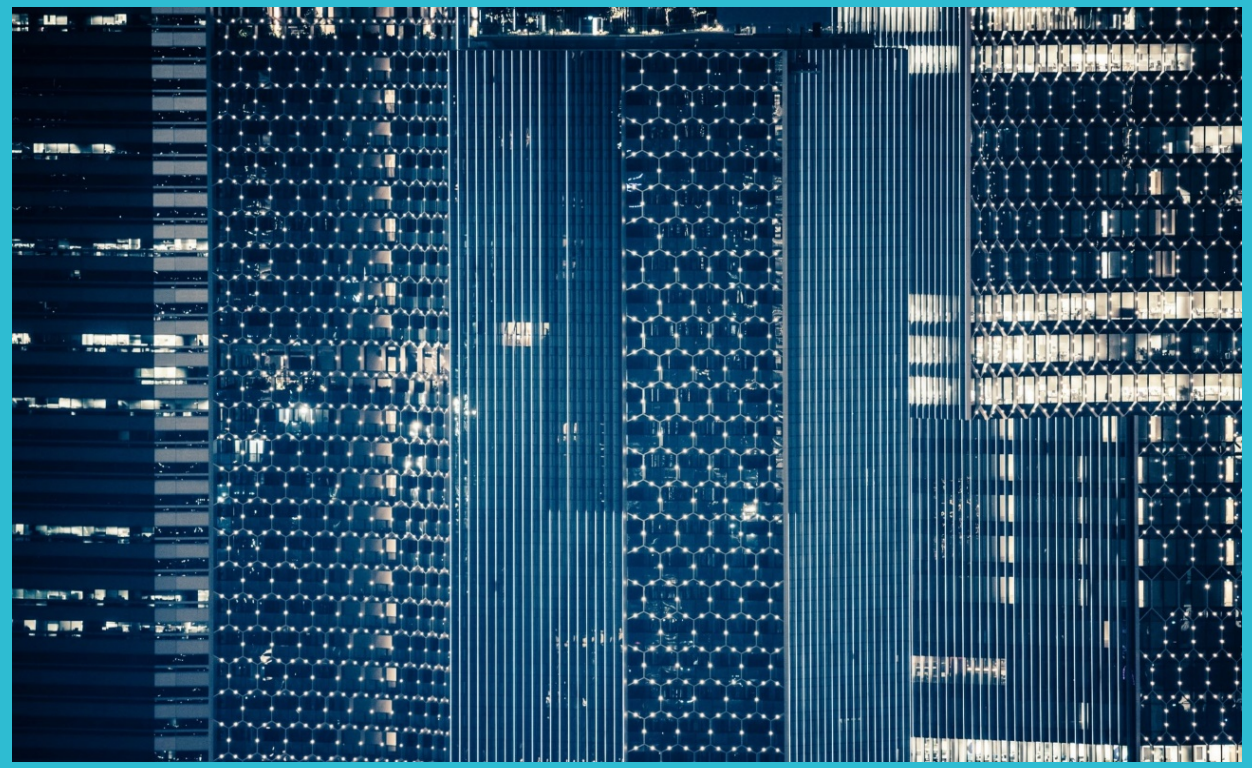
Step 6: Apply, Rinse, Repeat

- Prudent employers will periodically review, update, and re-implement all the (updated) privacy and data security policies.

- Remember to involve employees in this process!

PRIVACY LAW UPDATE

Emily M. Maass
Attorney



Current Landscape of Privacy Law

LANE POWELL

Pre -2018

- **HIPAA** (health care)
- **Graham -Leach Bliley** (finance)
- **PCI DSS** (payment processing)
- **COPPA** (children's online privacy)
- **TCPA & CAN-SPAM** (telecom & marketing)
- **FTC** (deceptive practices re consumer personal information)

2018

- **GDPR** (EU General Data Protection Regulation)
- **CCPA** (California Consumer Privacy Act)

2019

State Legislation

- Hawaii
- Maryland
- Massachusetts
- Mississippi
- New Mexico
- New York
- Nevada
- North Dakota
- Rhode Island
- Washington

Washington

- Washington Privacy Act
- Data Breach

Oregon

- IoT
- Data Breach
- Possible last minute data privacy bill to be introduced late in 2019 legislative session

General Data Protection Regulation

Effective Date: May 25, 2018

Applies to:

- Businesses, nonprofit organizations, charities and educational institutions that collect or process data of EU residents and individuals physically located within the EU at the time the data is collected or processed.
  - 250 or more employees, or
  - Fewer than 250 employees, but its data processing:
    - impacts the rights and freedoms of data subjects,
    - is more than occasional, or
    - includes certain types of sensitive personal data.

Does not apply to:

- Non-EU companies engaging in general global marketing.
- Non-EU companies making no effort to market in the EU or monitor the behavior of EU residents.
- European Union resident traveling in the US.
- Purely personal or household activity (e.g., collecting contact info to organize a family gathering).

Enforcement:

- Administrative fines of up to:
- €20 million or 4% of the organization's global annual revenue, whichever is greater
- Or €10 million or 2% of the organization's global annual revenue, whichever is greater.

LANE POWELL

General Data Protection Regulation

Data Subject Rights —Includes Employees

The GDPR provides data subjects with certain fundamental privacy rights including:

- Right to transparency (the right to be informed about the collection and use of one's personal data).
- Right to access their personal data.
- Right to object to the processing of their personal data.
- Right to restrict the processing of their personal data.
- Right to rectification.
- Right to erasure ("the right to be forgotten").
- Right to data portability.

California Consumer Privacy Act of 2018

Effective Date: January 1, 2020

Applies to:

- Any business that offers products or services to CA residents and collects their personal information, regardless of the location of the business, and:
  - has $25 million or more in annual gross revenues;
  - possesses the personal data of 50,000 or more consumers, households, or devices; or
  - earns more than 50% of its annual revenue from selling consumers' personal data.

Does not apply to:

- To nonprofit organizations.
- If every aspect of a business's collection/sale of PI takes place wholly outside of California.
- Sale to/purchase from a consumer reporting agency.
- De-identified or aggregated PI.
- PI covered by HIPAA or the California Confidentiality of Medical Information Act.
- PI covered by Gramm-Leach-Bliley Act or the California Financial Information Privacy Act.

Enforcement:

- AG regulations due July 1, 2020
- Enforceable by AG starting July 1, 2020
- Subject to a 30-day cure period
- Civil penalty up to $2,500 per violation or $7,500 per intentional violation, plus injunction

LANE POWELL

California Consumer Privacy Act of 2018

Effective Date: January 1, 2020

Applies to:

- Any business that offers products or services to CA residents and collects their personal information, regardless of the location of the business, and:
  - has $25 million or more in annual gross revenues;
  - possesses the personal data of 50,000 or more consumers, households, or devices; or
  - earns more than 50% of its annual revenue from selling consumers' personal data.

Does not apply to:

- To nonprofit organizations.
- If every aspect of a business's collection/sale of PI takes place wholly outside of California.
- Sale to/purchase from a consumer reporting agency.
- Deidentified or aggregated PI.
- PI covered by HIPAA or the California Confidentiality of Medical Information Act.
- PI covered by Gramm-Leach-Bliley Act or the California Financial Information Privacy Act.

Enforcement:

- AG regulations due July 1, 2020
- Enforceable by AG starting July 1, 2020
- Subject to a 30-day cure period
- Civil penalty up to $2,500 per violation or $7,500 per intentional violation, plus injunction

LANE POWELL

California Consumer Privacy Act

Consumer Rights

The CCPA provides consumers with the following rights:

- Right of Access.
- Right of Deletion.
- Right to Know What PI Information is Collected & Whether PI is Sold.
- Right to Opt Out or Opt In.
- Right of Equal Service.

Who/What is Protected?

LANE POWELL

- "Consumer" = A natural person who is a California resident.
  - Currently includes employees.
- Personal Information ("PI") relating to any CA resident, regardless of a business's relationship to the individual.
- PI = *very broad*
  - **Any information that** identifies, relates to, describes, references, **is capable of being associated with**, or could reasonably be linked directly or indirectly with **a particular *consumer* or *household***. It includes not just the standard (name, address, etc.), but also items that indirectly identify a unique person, such as aliases, IP addresses, account names, etc. It also includes commercial information such as records of products or services purchased or considered, or other purchasing histories or tendencies, and geolocation data (i.e., internet activity information that is collected by online tracking services).

What About Employees?

- CCPA does not apply to PI collected by a business in certain limited employment-related contexts **until January 1, 2021**
- Includes personal information:
  - Collected from job applicants, employees, business owners, directors, officers, medical staff, or contractors and used solely in that context
  - Collected for emergency purposes and used solely in that context
  - Necessary to administer benefits
- Limitations
  - May exercise "Right to Know" in employment context
  - May bring a limited private right of action in employment context
  - Nonemployment uses of employee personal information

Other Uses of Employee Data

Statutory exceptions do not necessarily cover all manner of data processing by employers.

- B2B transactions & partnerships
- Fringe benefits & perks programs
- Organizational statistics
- Workplace culture & employee morale analytics
- Partnerships with other organizations
- Selling or sharing data

		CCPA	GDPR
CONSUMER RIGHTS	Right of Transparency / Right of Notice	✓	✓
	Right of Access	✓	✓
	Right to Opt-Out of PI Processing		✓
	Right to Opt-Out of PI Sale	✓	✓
	Right to Restrict ("Selective Opt-out")		✓
	Right to Object		✓
	Right to Correct PI		✓
	Right to Erasure/Deletion	✓	✓
	Right to Data Portability	✓	✓
	Right of Equal Service	✓	
COMPLIANCE	Privacy by Design		✓
	Stated Lawful Basis		✓
	Appoint a Data Protection Officer		✓
	Dedicated Link: "Do Not Sell My Personal Information"	✓	
	2+ Methods to Submit Consumer Requests	✓	
	Responsible for Proper Handling of PI by Others	✓	✓
	Specific Permissions to Process PI of Children	✓	✓
	Information provided free of charge	✓	✓
	Mandatory provisions in privacy policy/other policies	✓	✓
	Mandatory provisions in 3rd party contracts	✓	✓
	Data Breach Response Protocols	✓	✓
ENFORCEMENT	Warnings/Notice	✓	✓
	Audits		✓
	Government Enforcement	✓ (Attorney General)	✓ (Member State Supervisory Authority)
	Fines	✓ ($2,500 per violation/ $7,500 per intentional violation)	✓ (Up to €10 million or 2% annual worldwide turnover/up to €20 million or 4% annual worldwide turnover)
	Private Right of Action	✓ ($100 to $750 per consumer per incident or actual damages)	✓ (Actual damages caused by failure to comply with GDPR provisions)

Responding to Employee Requests

- **Receive the request**
  - Standard forms; email, mail, phone, etc.
- **Identity Verification**
- **Categorize the request:**
  - Access
  - Deletion
  - Opt-out/Restrict
  - Data Portability
  - Information about PI sold (CCPA only)
  - Rectification (GDPR only)
- **Locate the requested data**
- **Fulfill request**
- **Respond**
  - Free of charge
  - Within 45 days (CCPA) or 30 days (GDPR)
  - In a concise, transparent, intelligible and easily accessible form, using clear and plain language
- **Recordkeeping**

- **Extensions of Time**
  - CCPA permits up to 90 day extension to respond to complex requests
  - GDPR provides for a two month extension "where necessary, taking into account the complexity and number of the requests."
  - Must inform the employee of the extension and give a reason within the initial deadline
- **Refusing disclosures**
  - Unable to verify requester's identity
  - Request is unfounded or excessive (GDPR)
  - More than two requests in a 12-month period (CCPA, does not apply to deletion or opt-out)
- **Limiting Disclosures**
  - Avoid adversely affecting the rights of others
  - Compliance with laws
  - Legal necessity

Case Study: Oregon Trade Exchange

Oregon Trade Exchange is a retailer headquartered in Portland.

OTE has a team of employees who work remotely, including an employee who has works for OTE from his home in San Francisco.

In 2020, OTE eliminates the employee's position.

The employee sends his former supervisor an email requesting "copies of all the data you have about me, and I demand that you delete all personal information you have about me."

How is OTE required to respond?

Case Study: Oregon Trade & Exchange

LANE POWELL

Does the CCPA apply?

- Applicability thresholds: $25 million revenue or 50,000 consumers or households.
- Employment-related personal information: January 1, 2021.
- Personal information collected, used or sold for other purposes.

How must OTE respond to this request?

- Full or partial exemption until January 1, 2021
- Right to Access
- Right to Deletion
- Verify employee's identity
- 45 days
- Option to extend up to an additional 90 days if the request is complex
- Beware the "look back"

Case Study: Oregon Trade Exchange, Intl.

This time, OTE's remote employee lives in France.

The employee submits a Data Subject Access Request to "make all of my personal data available to my new employer and then delete all personal information you have about me."

How is OTE required to respond?

Case Study: Oregon Trade Exchange, Intl.

LANE POWELL

Does the GDPR apply?

- Applicability thresholds
- EU resident
- No exemption for employees or employment related personal data

How must OTE respond to this request?

- Full or partial exemption until January 1, 2021
- Right to Data Portability
- Right to Deletion
- Verify employee's identity
- 30 days
- Option to extend response for two months, refuse disclosure if request is excessive, or limit disclosure to protect the rights of others.

The Future of Privacy Regulation: 5 Year Outlook

Two models: GDPR & CCPA	Privacy built-in
	Comprehensive consumer rights
Industry & Consumer Lobbies	Private right of action
	Aggressive regulatory enforcement by states
Enforcement	Private Right of Action
	Federal legislation would bring consistency and limit state AGs
Federal Legislation	Gain a competitive edge by embracing privacy as a value

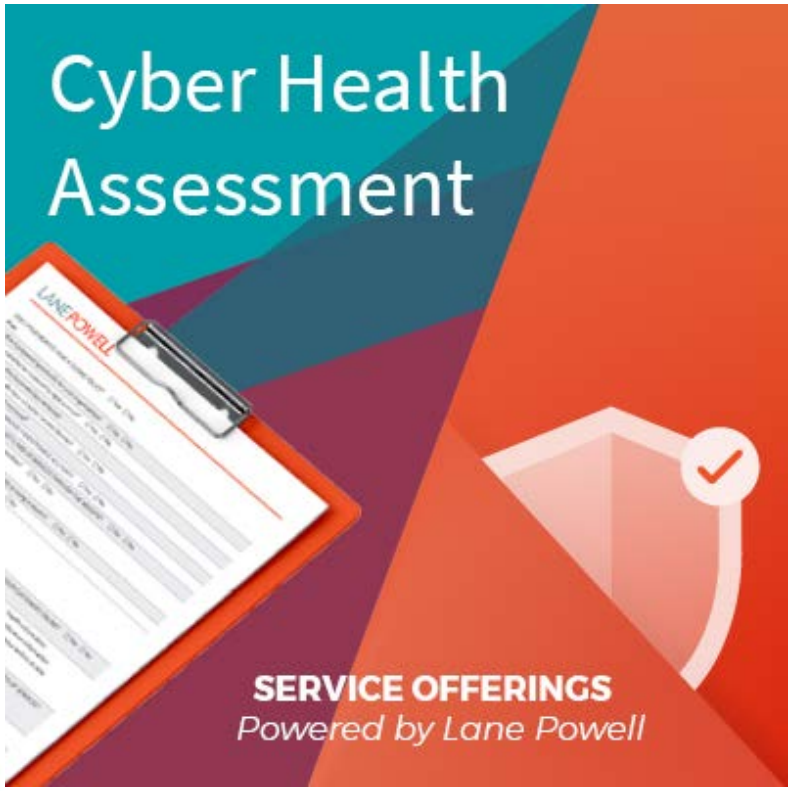
When in Doubt
Best Practices

Transparency.	A workplace culture of sensitivity to data privacy.
Consent.	Treat essential employee information as highly sensitive.
Accessibility.	Treat non-essential information as consumer personal information.
Choice.	Careful use of employee analytics software and tools.
	Remember the spirit of the law.
Minimize Impact.	No penalties.

Using Data for Good

All companies are tech companies.	Data is a business asset.
	Data mapping.
	Data hygiene.
Demand for innovative solutions.	Commercial relationships.
	Commercial contracts.
Tailored solutions.	Client confidence.

It never hurts to go in for a checkup…



Free one-hour consultation to assess a company's data landscape

Evaluate risks and liabilities

Build recommended suite of legal services

Develop pricing structure reflective of need

Meet Our Privacy & Data Security Team

We provide full service counseling at every stage of the data lifecycle. Our attorneys are leading experts in state, federal and international statutes and regulations including GDPR, CCPA, and WPA, alongside decades of experience with HIPAA considerations, consumer financial data including Graham-Leach Bliley applicability, and marketing practices under CAN-SPAM and the TCPA.

Our experienced and technologically savvy attorneys craft tailored strategies to assist clients in effectively and efficiently minimizing legal and reputational risk related to the collection, use, storage and loss of data.

We help clients with :

- Tailored strategies for comprehensive privacy law compliance.
- Solutions for startups to enterprise companies
- Policy development and implementation.
- Website readiness.
- SaaS agreements, cloud-based service contracts, DevOps and other technology product and service offerings.
- Risk evaluation
- Data breach response planning.
- Incident response management.
- Representation in civil lawsuits and regulatory investigations.
- Tabletop exercises and corporate training.

Julie Engbloom

Darin Sands

Peter Fisk

Emily Maass

Brandon Archuleta

Jeff Brecht

Let's Connect

dataprivacy@lanepowell.com

Jeff Duncan Brecht
Shareholder
503.778.2162
brechtj@lanepowell.com

Emily M. Maass
Attorney
maasse@lanepowell.com
503.778.2149

LANE POWELL