THE CHANGING LANDSCAPE OF PRIVACY & CYBERSECURITY

CLARISSA BENAVIDES

MANAGING COUNSEL – TOYOTA FINANCIAL SERVICES

12.15.22

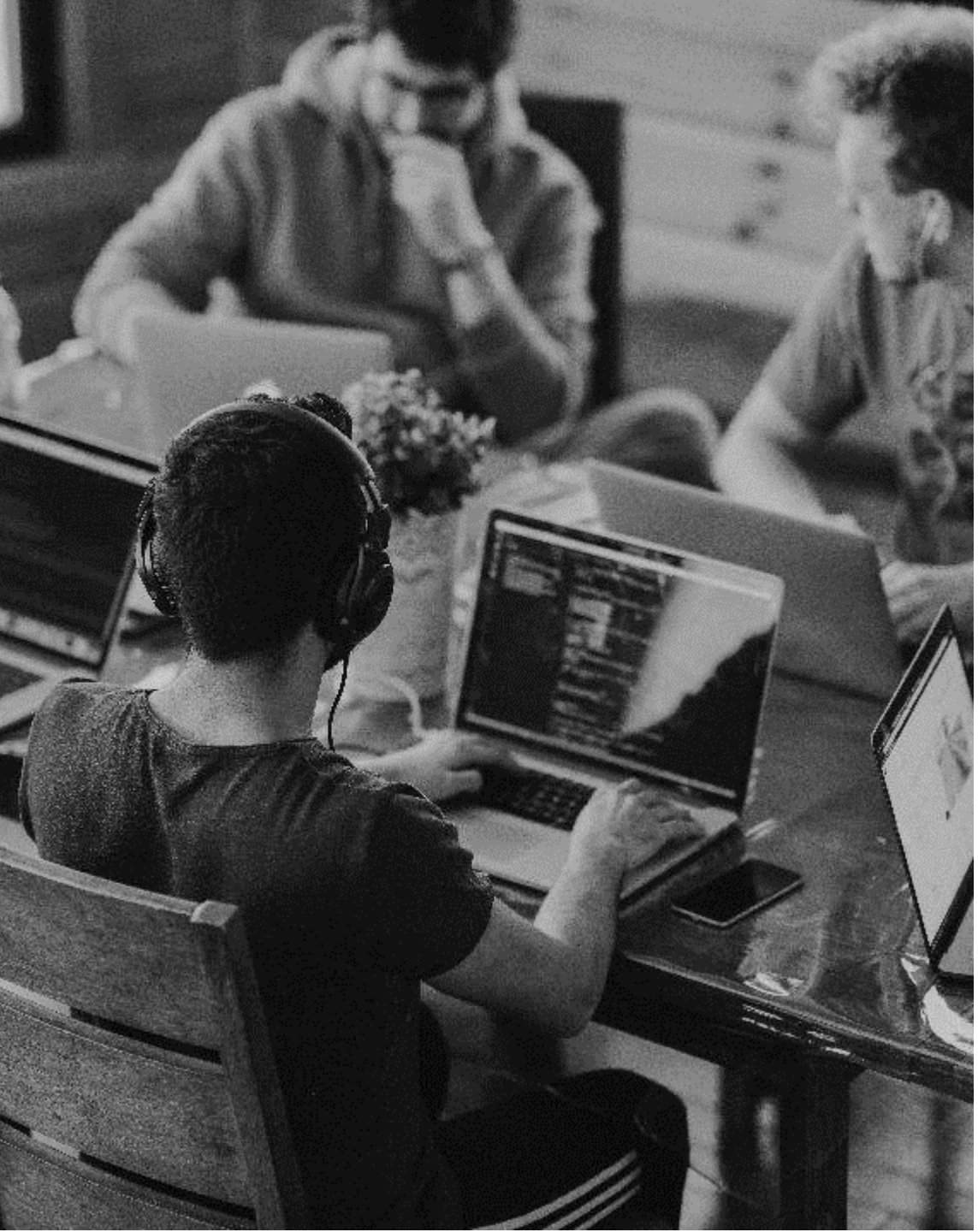
AGENDA

PRIVACY LANDSCAPE

TEXAS PRIVACY LAWS

CYBERSECURITY

PRACTICAL TIPS



PRIVACY VS CYBERSECURITY

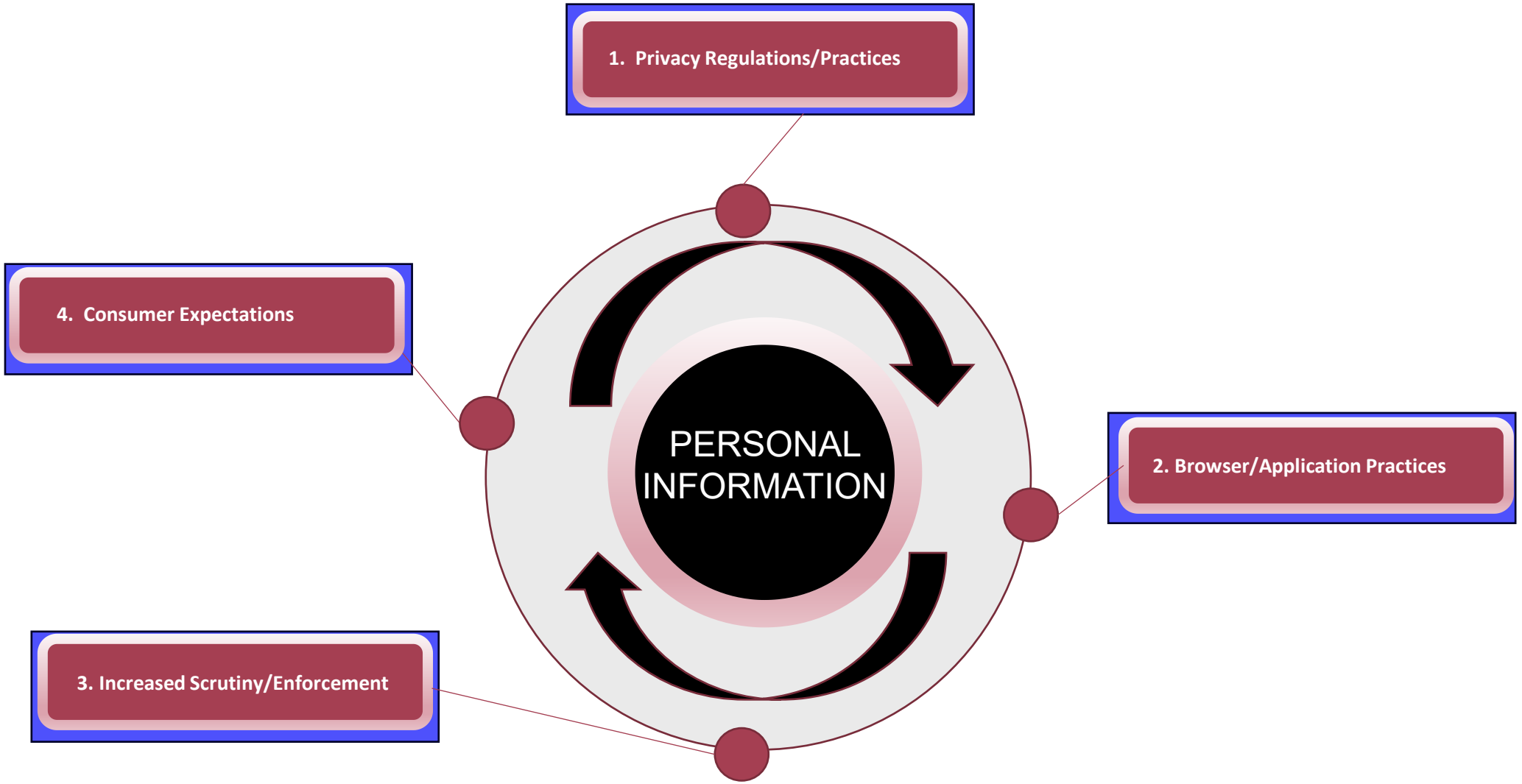
DEFINED

Privacy is how you use personal data vs ***Security*** is how you protect personal data.

Personal Data means all information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual (“Data Subject”) or household.

Examples include: name, address, email, SSN, bank account number, photos/videos, credit card numbers, usernames & passwords and IP addresses.

PRIVACY LANDSCAPE



PRIVACY LAW HISTORY

1999	2018	2020/2021
GLBA HIPPA FERPA	GDPR CCPA	CA/CT VA/CO UT
SECTORAL Initially, privacy laws applied to a specific industry like financial institutions, medical facilities/practices and educational institutions.	EUROPE & CALIFORNIA In 2018, Europe enforced the first comprehensive privacy law for its residents, and this had impact on international Companies. It also began the trend for governments in the US to care about privacy and California was the first to pass a comprehensive privacy law in the US for its residents in 2018.	ADDITIONAL STATES In 2020, CA initial privacy law goes into effect. In 2021, CA enhanced and 4 additional states passed their own comprehensive privacy law. Each of the new laws will go into effect in 2023.

PRIVACY LANDSCAPE

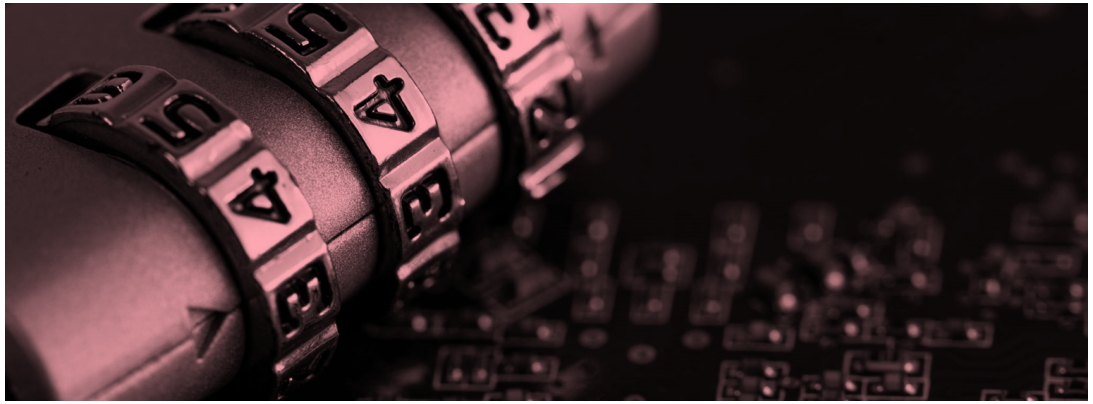
Consumer Rights

- Right to Know
- Right to Correct
- Right to Delete
- Right to Data Portability
- Right to Opt Out of Sale
- Right to Opt Out of Targeted Advertising and/or Profiling
- Right to Non-Retaliation
- Right to Limit Use and Disclosure of SPI
- Right to Consent to process SPI
- Right to Appeal
- Private Right of Action

Business Obligations

- Data Minimization
- Purpose Limitation
- Reasonable Data Security
- Privacy Notice
- Limit Use of SPI
- Consent for SPI
- No Discrimination
- Correction and Deletion Process
- Appeal Process
- Contractual Requirements
- Data Protection Assessments

CHANGING PRACTICES & EXPECTATIONS



BROWSER/APPLICATION PRACTICES

- Safari, Firefox and Google will or already block all third-party tracking cookies
- Apple iOS 14.3 requires all Apps on its App Store to include a privacy nutrition label describing the App's privacy practices
- Apple iOS 14.5 ask users whether they consent for the App "to track your activity across other companies' apps and websites."

CONSUMER EXPECTATIONS

- Increased awareness of privacy concerns due to Cambridge Analytica, Google tracking and Smart Devices snooping has evolved consumer expectations for privacy
- Customers won't engage with companies they don't trust. A majority will stop buying/ using the service due to privacy
- In fact, customers strongly associate privacy with trust. Majority of consumers will share their data with brands they do trust

2022 ENFORCEMENT TRENDS

SEPHORA

- $1.2 Million
- California Attorney General
- Sephora (1) failed to disclose that it sells data; (2) engaged in the unlawful sale of personal information, including exchanging data with third parties for analytics information; (3) failed to post a “Do Not Sell My Personal Information” link on its website and homepage; and (4) failed to respond to or process consumer opt-outs in accordance with global privacy controls

JP MORGAN

- $125 Million
- U.S. Securities & Exchange Commission
- Company had recordkeeping failures, specifically, employees communicated about business matters on personal devices, including text messages and personal emails and these records were not preserved as required under law.
- Additionally, they will invest in implementing “robust improvements to its compliance policies and procedures.”

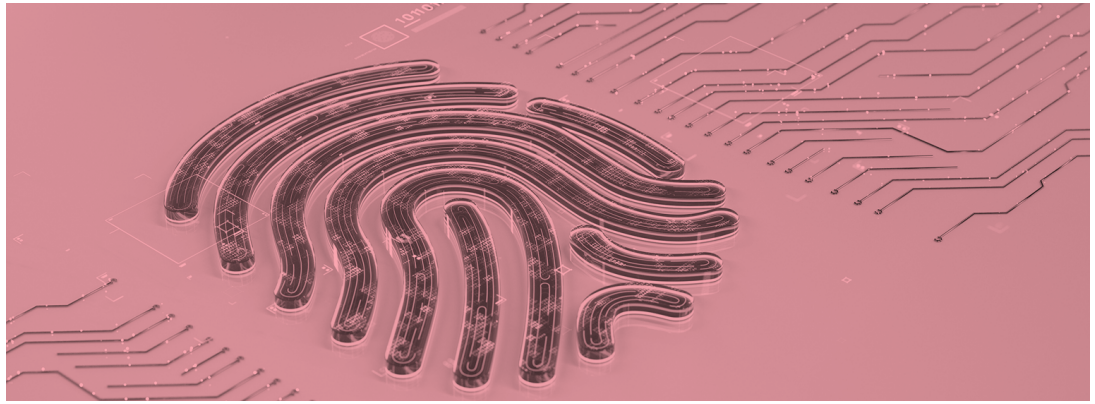
META/FACEBOOK

- $37.5 Million
- Civil Class Action Suit
- Meta violated users’ privacy — and the company’s own policies — by using location data to target ads.
- The class consists of Facebook users who had switched off “location services” on their phones, but still had their locations “inferred” by Meta’s use of their IP addresses.

WILL THERE BE A FEDERAL PRIVACY LAW?

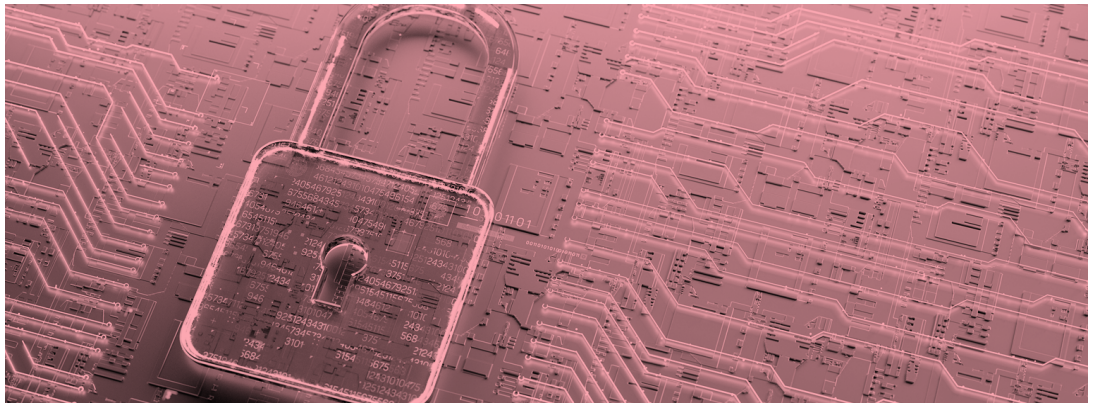
ADPPA

TEXAS LAWS



CAPTURE OF USE OF BIOMETRIC IDENTIFIER

- CUBI codified in Tex. Bus. & Com. Code Sec. 503.001
- Applies to all private entities that use biometric identifiers for a commercial purpose including employers.
- Biometric Identifier includes retina/iris scan, fingerprint, voiceprint or record of hand/face geometry
- Requires Notice and Consent before capturing biometric identifier. But neither notice nor consent must be in writing.
- Prohibited from selling, leasing or disclosing unless meet exception



TEXAS BREACH STATUTE

- Codified in Tex. Bus. & Com. Code Sec. 521.053
- Applies to any person who conducts business in Texas and owns or licenses computerized data that includes sensitive personal information
- Sensitive Personal Information includes (1) an individual first name or initial and last name in combination with SSN, DLN, account/debit/credit number with security code or password or (2) information that identifies an individual's physical/mental condition or provision of health care
- Breach when have unauthorized acquisition that compromises the security, confidentiality or integrity of the data

CYBER TRENDS

MORE AGGRESSIVE RANSOMWARE TACTICS

Shame sites, DDOS attacks, direct contact with employees by threat actors

THREAT ACTORS TARGETING SPECIFIC INDUSTRIES

Law firms, consulting companies, health care

INCREASING REGULATION ON BREACH PREVENTION AND REPORTING

Critical infrastructure, public companies (SEC), financial institutions

TOUGHER UNDERWRITING ON CYBER-INSURANCE POLICIES

Especially around ransomware

VENDORS & PLAN

THIRD PARTIES

- Have significant access to systems & data
- Have less stringent cybersecurity measures & more vulnerable to phishing
- Identify if they have a plan to test their protocols, document efforts to fix vulnerabilities and communicate best practices to employees
- Monitor access to internal data & implement alerts for unauthorized access by them
- Vendor contract should include provisions obligating the vendor to report breach incidents and specific security requirements

INCIDENT RESPONSE PLAN

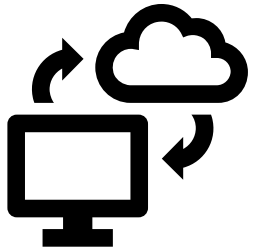
- Develop a plan with contacts and roles
- Conduct a tabletop exercise to ID gaps
- Secure cybersecurity insurance & understand your policy/needs
- First priority – contain the damage and then get company restored
  - Do you have backups?
  - Is data encrypted?
- Share information on a need to know and determine whether will need to provide notice of breach
- Develop templates for any notice for regulators

INCIDENT TEAM

- Legal
- Outside counsel
- Forensic expert
- IT
- PR
- Remember, cyber security is not a technical problem but a major risk facing all organizations

PRACTICAL MITIGATION TIPS

SECURE NETWORK

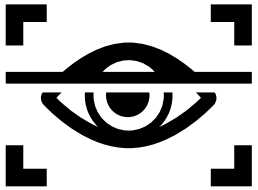


Launch updates for any device (doorbell/cameras)

Create unique wi-fi/router names

Run penetration testing

LIMIT ACCESS & RETENTION



Limit access on a need-to-know basis

Have a protocol to quickly remove access from terminated employees

Only keep data that is needed and limit collecting PI

TRAIN

Your employees on how to detect phishing

Establish protocols for verification before transferring $ or sensitive info

TAKEAWAYS

IDENTIFY PERSONAL DATA

- Identify where you collect personal data (intake form, bank account numbers, medical information, etc.)
- Determine who has access and if properly secured
- Establish a retention schedule for personal data

PROVIDE TRANSPARENCY

- Determine if any of the laws apply
- Understand your role/business to assess if need to make changes (notice/consent)
- Treat personal data as you want others to treat it

STAY CURRENT & TRAIN STAFF

- Do you share personal data with new entities
- Visit CISA for latest cyber trends and tips
- Train staff and practice responding to an incident

QUESTIONS

THANK YOU

THANK YOU

CLARISSA BENAVIDES

+1 (469) 588-6010

Clarissa.Benavides@ toyota.com

QUESTIONS