2020 UPDATE ON DATA PROTECTION AND PRIVACY LAWS, TRENDS, AND COMPLIANCE RECOMMENDATIONS

MAY 13, 2020
PRESENTATION TO:

THE ACC MID-AMERICA CHAPTER

BY:

LAURA CLARK FEY, Esq
Privacy Law Specialist (IAPP)
CIPP/US, CIPP/E, CIPM, FIP
Fey LLC | Leawood, KS

Tailored to You

"I wrote this next song using your personal information, so I know you'll like it."

Agenda

- High-Level Current State Overview
- California Consumer Privacy Act and Class Action Trends
- Biometric Data Privacy Laws and Class Action Trends
- What Else is New?
- What Do We Have to Look Forward to?

HIGH-LEVEL CURRENT STATE OVERVIEW

Plethora of Data Privacy and Protection Laws

- Current State
  - **Global**: Multitude of Laws in Over 100 Countries
  - **U.S.**: Patchwork Quilt of Hundreds of Federal, State, and Now City Data Privacy and Protection Laws

Giving Rise to a Host of Widely Varying Legal Obligations

- Information Security
- Data Integrity
- Notice/Transparency
- Consent/Lawful Basis for Processing
- Limitations on Data Usage
- Limitations on Transfer and Sale
- Third-Party Contracting
- Data Subject Rights
- Restrictions on Electronic Marketing Communications
- Data Breach Notification and Incident Management
- Data Destruction
- Accountability Practices/Recordkeeping

Significant Recent Increase in Data Privacy and Protection Regulatory and Legislative Activities

- Worldwide
  - Significantly Increased Regulatory Activity in Recent Years (Particularly in the EU and in Canada, Where Data Protection Authorities are Among the Most Active in the World) and More Global Coordination in Regulatory Enforcement Activities
- In the U.S., Where Data Privacy and Security Investigations and Inquiries for Significant Data Breaches Now Often Involve:
  - Federal Regulators
  - State Regulators
  - Members of Congress
  - State Legislators

The Plaintiffs' Bar is Increasingly Interested in Data Privacy and Protection Class Actions

- Multitude of Data Privacy and Protection Class Actions Filed in 2019 and Early 2020
- More Filings are Anticipated This Year (and Moving Forward) as New Technologies Give Rise to New Privacy Concerns and New Breaches, and as Data Privacy and Protection Expectations Continue to Increase

- ***"There is a growing campaign by the plaintiffs' bar to target data privacy and security in the hopes of striking it rich in a new goldmine on the level of the asbestos litigation on the 1970s, 1980s, and 1990s."***

  – U.S. Chamber of Commerce Institute for Legal Reform

General Counsel Anticipate Data Privacy and Protection Class Actions Will be the "Next Wave"

- ***54% of General Counsel Predict Data Privacy and Security Will be the "Next Wave of Class Actions," With 2/3 of Companies Expressing Specific Concern About the CCPA***

  -2019 Carlton Fields Class Action Survey of General Counsel and Senior In-House Attorneys

- ***"When the legislators in [] states pass laws that allow consumers to bring private rights of action regarding [personal] data issues, companies are rightly concerned. California, in particular, is a place where class actions are filed more than in any other state in the nation. California is an issue; Illinois is an issue, and other states are starting to copy those laws that are probably going to get passed in the next three to five years."***

  -Julianna McCabe, Director of the National Class Action Survey

CALIFORNIA CONSUMER PRIVACY ACT AND CLASS ACTION TRENDS

Key Legal Obligations

- Obligations Directly Imposed by the CCPA:
  - Notice/Disclosure
  - Consent for Selling of Children's Data
    - 13-16: Children's Consent Acceptable
    - Under 13: Parental Consent Required
  - "Do Not Sell My Personal Data" Webpage (Linked in Privacy Policy)

Key Legal Obligations

- Obligations Directly Imposed by the CCPA:
  - Data Subject Rights Compliance:
    - Access
    - Portability
    - Erasure/Deletion
    - Sale Opt-Out/Prevention
    - Non-Discrimination

Recent Regulatory and Legislative Actions

- Third Draft of CCPA Regulations Issued
- AG Advised Enforcement Will Begin on July 1 (Regardless of COVID-19)
  - Enforcement of Regulatory Provisions May be Delayed
- AG Considers Enforcement Alternatives (*e.g.*, Empowering District Attorneys and City Attorneys to Bring Enforcement Actions)

CCPA Class Action Trends

- 19 California Class Lawsuits Alleging CCPA Violations to Date

- Types of Cases:
  - Causes of Action Based on Data Breach Under CCPA
  - Cause of Action Based on CCPA Data Privacy Violations (*e.g.*, Alleging No Notice at Collection)
  - No CCPA Cause of Action, But CCPA Referenced in Other Contexts (*e.g.*, in Actions Brought Under Unfair Competition Law)


712

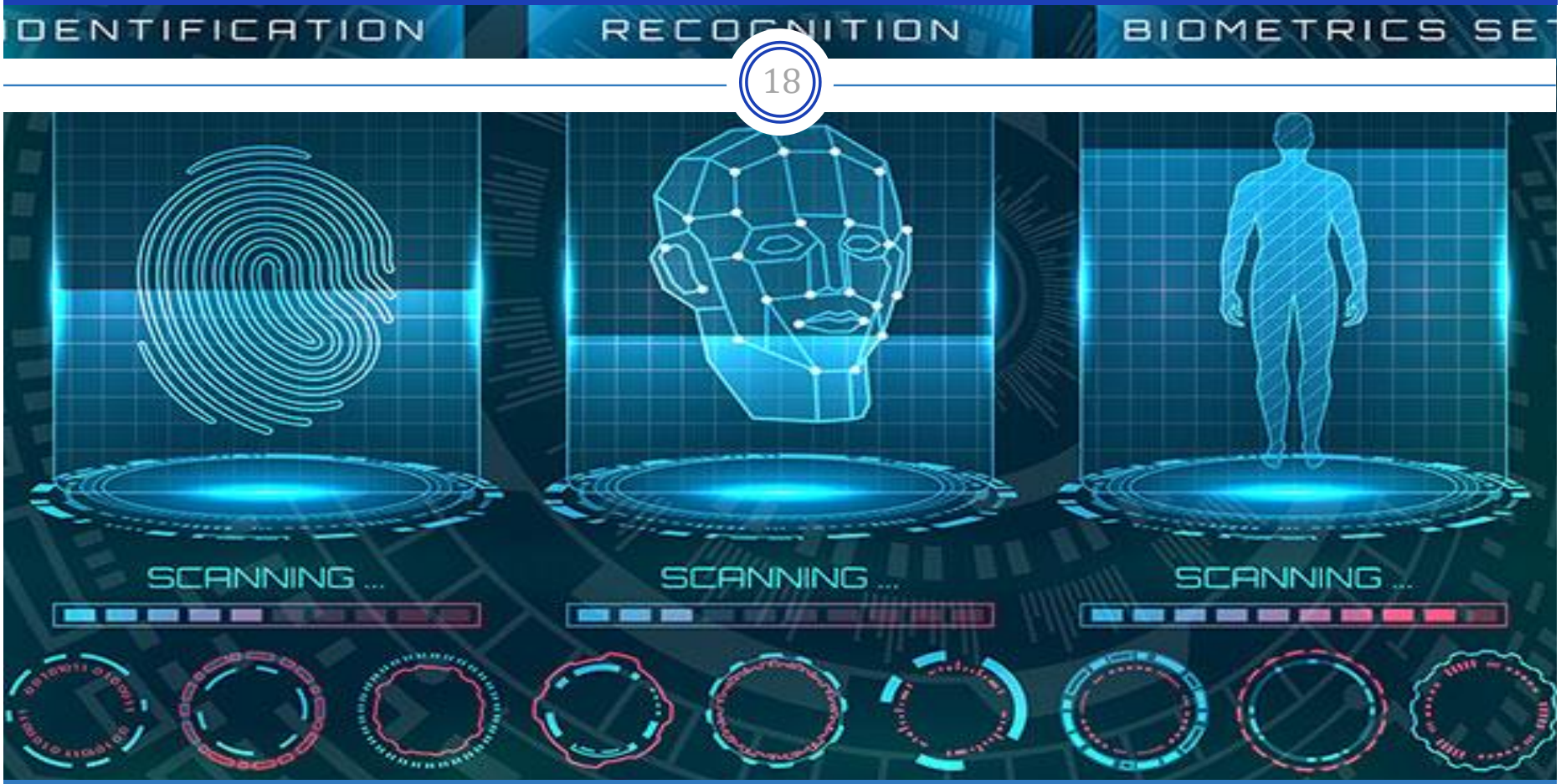
CCPA Class Action Trends

- Exemplar Cases:
  - Barnes v. Hanna Andersson and Salesforce.com
  - Sheth v. Ring LLC
  - Cullen v. Zoom Video Communications
  - Burke v. ClearviewAI

Top 5 Compliance and Risk-Reduction Recommendations

- Confirm Reasonable Information Security Program, including Implementation of CIS Critical Security Controls and Security Incident Response Procedures
- Prepare Data Map/Data Flows
- Update Privacy Notice and Vendor/Service Provider Contracts
- Draft and Implement Consumer Rights Procedures
- Incorporate Arbitration Provisions and Class Action Waivers into Agreements

BIOMETRIC DATA PRIVACY LAWS AND CLASS ACTION TRENDS



U.S. Biometric Privacy Laws

- Illinois
  - Applies to All Biometric Information
  - No Collection Without Written Notice and Release
  - No Disclosure for Profit
  - Other Types of Disclosure Permitted Only If:
    - Consent Received
    - For Completion of Requested/Authorized Financial Transaction
    - Required by Law
    - Pursuant to Valid Warrant or Subpoena
  - Mandates Reasonable Security Measures and Requires Written Retention/Destruction Policy
  - Provides for Private Right of Action

U.S. Biometric Privacy Laws

- Texas
  - Applies Only to Biometric Identifiers (*i.e.*, Records of Biometrics)
  - No Collection Without Notice and Release (Not Required to be Written)
  - No Disclosure for Profit
  - Sale or Disclosure Only If:
    - Consent Received
    - For Completion of Requested/Authorized Financial Transaction
    - Required by Law
    - Pursuant to Valid Warrant or Subpoena
  - Requires Reasonable Security
  - Strict Data Destruction Requirements
  - No Private Right of Action

U.S. Biometric Privacy Laws

- Washington
  - Applies Only to Biometric Identifiers Collected for Commercial Use that are Enrolled in a Database; Does Not Apply to Facial or Hand Geometry Scans
  - May Enroll Biometric Identifiers in Database for Commercial Purpose With One of the Following:
    - Notice
    - Consent, or
    - Mechanism to Prevent Subsequent Use for Commercial Purpose
  - Sale or Disclosure Only If Consent Received
  - No Private Right of Action

Biometric Data is Increasingly Covered by Broader Privacy Laws

- **Nebraska:** Unique Biometric Data, Such as a Fingerprint, Voice Print, or Retina or Iris Image, Covered by Data Breach Notification Law
- **California:** Biometric Data is Personal Information (CCPA)
  - Biometric Data: "An individual's physiological, biological or behavioral characteristics, including an individual's DNA, that can be used singly or in combination with each other or with other identifying data, to establish individual identity"
- **EU:** Biometric Data is "Special Category of Personal Data" (GDPR)
  - Biometric Data: "Personal data resulting from specific technical processing relating to the physical, physiological, or behavioral characteristics of a natural person, such as facial images or dactyloscopic (fingerprints) data."

Key Legal Obligations Arising from Biometric Privacy Laws

- Written Notice of Collection
- Individual Consent to Collection
- Consent for Disclosure or Sharing for Authorized Purpose
- Reasonable Information Security
- Written Retention and Destruction Policy

Recent Regulatory and Legislative Actions

- **San Francisco:** 2019 Ban on Governmental Use of Facial Recognition Technology
- **Illinois:** 2019 Bill to Eliminate Private Right of Action Failed
- **Washington**: Bill Governing Facial Recognition Technology Providing Consumers with Opportunity to Access, Correct, Delete and Transfer Data Passes Both Chambers of the House
- **Arizona and Florida:** Biometric Privacy Legislation Introduced in 2019, But Failed to Pass
- **Massachusetts:** Broad Consumer Privacy Bill Introduced Covering Biometric Data; Committee Reviewing Bill Issued Study Order on 2/5/20

Class Action Trends

- **Surge of BIPA Actions, With More to Come:** All Industries Targeted in Torrent of Class Actions Filed Under BIPA After Illinois Supreme Court and 9th Circuit Decisions Significantly Reduced the Burden to State Actionable Claims
  - Filing Location: Majority Filed in Cook County, Illinois
  - Most Targeted Industries to Date: Business Services (*e.g.*, Staffing, Logistics, Janitorial); Healthcare; Manufacturing; Hospitality; Retail; Software and Technology
- **Plaintiffs' Attorney Commentary:** "Biometrics is one of the two primary battlegrounds, along with geolocation, that will define our privacy rights for the next generation."

  -Jay Edelson, Edelson PC

Class Action Trends

- Key Cases:
  - **Rosenbach v. Six Flags Entertainment Corp.:** Actual Damages Not Required (Ill. S. Ct.)
  - **Patel v. Facebook:** Use of Facial Recognition Software in Photo Tagging Without User Consent is Concrete Harm Sufficient to Confer Article III Standing (9th Circuit)
  - **Peatry v. Bimbo Bakeries:** Denied Remand Because Damages Over $5M Possible If Each Scan Deemed to Constitute Single Violation (N.D. Ill.)
  - **Rogers v. CSX Intermodal Terminals:** Privacy Right Encompasses Right to Voluntarily Provide Biometric Data Only After Receiving Proper Notice and Providing Consent (N.D. Ill)

Top 5 Compliance and Risk-Reduction Recommendations

- Provide Written Notice and Obtain Written Consent/Release (If Required) Prior to Collecting or Disclosing Biometric Data
- Update Consent Processes and Third-Party Vendor Contracts
- Directly Address BIPA in Collective Bargaining Processes
- Establish Good Practices for Accessing, Storing, Transferring, and Safeguarding Biometric Data
- Draft, Implement, and Maintain Publicly-Available Data Retention and Destruction Policy

WHAT ELSE IS NEW?

New York Stop Hacks and Improve Electronic Data Security Act (SHIELD)

- **Expanded Definition of "Breach":** Now Includes Unauthorized Access of Computerized Data in Addition to Unauthorized Acquisition

- **Expanded Territorial Scope**: Applies to Any Person or Business That Owns or Licenses a New York Resident's Data Regardless of Whether Conducts Business in New York

- **Expanded Notification Requirements and "Risk of Harm" Exception**: Must Provide Information to Affected Persons and Provide Public Agencies With Template of the Notice

New York Stop Hacks and Improve Electronic Data Security Act (SHIELD)

- **Enhanced Data Security Requirements**: Requires Adoption and Maintenance of Reasonable Administrative, Technical and Physical Safeguards to Protect the Confidentiality, Security and Integrity of Private Information
- **Enforcement**: Lies With the State AG; No Private Right of Action

Federal Privacy Law

- Many Failed Attempts Over the Years
- Congress Continues to Deliberate on Federal Privacy Legislation
- Issues to Debate are Narrowing
- Preemption Remains the Biggest Issue

COVID-19 Related Privacy Challenges

- Balancing Privacy Concerns Against Need to Protect Employees from Potential Infection
- Considering HIPAA Implications in Connection with Employer-Sponsored Health Plans
- Identifying and Complying with State Law Restrictions on Disclosure of Health Information
- Staying on Top of EEOC and Other Regulatory Guidance
- Addressing Increased Risk of Malware and Phishing Attacks in Connection with Working from Home

COVID-19: Test Nebraska Privacy Concerns

- State Senators Raise Privacy Concerns
- U. of Utah Professor: Data Collected "Could Ultimately be Far More Valuable than the Money the State is Paying to Implement [the] Programs."
- Governor Ricketts: "Your Data will Not be Sold, Either Individually or Aggregate. You can Feel Confident when You Sign Up Your Data will be Your Data."
- But Per News Reports: Privacy Policy Shows Personal Information May be Retained on File "Forever," and Can be Shared with Other Users.

COVID-19 Related Privacy Recommendations

- Limit Health Data Collection to Necessary Data Only
- Provide Notice and Obtain Consent Where Appropriate
- Examine and Consider Updating Internal and External Policies Regarding Data Collection
- Stay Up-to-Date on Relevant Laws, Regs and Rules
- Implement Reasonable Security Measures and Mechanisms for Handing COVID-19 Related Data
- Update Security Measures for Remote Workers and Train Employees on Key Risks

WHAT DO WE HAVE TO LOOK FORWARD TO?

Privacy Trends

- Continued Proliferation of U.S. and Global Privacy Regulations
- Continued Increase in Regulatory Enforcement Actions
- Continued Proliferation in Class Action Litigation
- Increasing Costs of Non-Compliance
- Increasing Client/Customer Demands
- Increasing Priority Placed on Strong Privacy Programs
- Increasing Challenges in Meeting Varying Obligations

More Laws

- More Laws on the Way
  - Over 3600 Bills Proposed in 2019 With Privacy as a Primary Key Word
  - After the California's Comprehensive Consumer Privacy Act Passed, Many States Proposed Similar Legislation; Nevada's Passed; Some are Still Pending; New Ones are Expected

Proposed CCPA Copycat Laws

- **Nebraska Consumer Data Privacy Act**:
  - In Committee; Very Similar to CCPA; No Private Cause of Action
- **New York Privacy Act (NYPA):**
  - Failed, but Speculation the Bill Will Make a Comeback; Bill Goes Further Than the CCPA by Placing a Fiduciary Duty on Data Collectors
- **Maryland Online Consumer Protection Act:**
  - Cross Committee; Many CCPA Similarities
- **Massachusetts Consumer Data Privacy Law:**
  - Study Order issued; Many CCPA Similarities; Includes Right for Consumers to Sue for Any Violation (without Demonstrating Loss of Money or Property)

California Privacy Rights Act

- **Alastair Mactaggart's Latest Ballot Initiative:** "[W]e've introduced a new initiative that will further protect our most personal information, increase fines for violating kids' privacy, create more transparency, and most importantly, establish an enforcement arm that truly looks out for consumers."
- Establishes New Enforcement Arm
- Requires Disclosure of Role of Automated Decision-Making
- Provides Enhanced Rights for Sensitive Personal Information
- Gives Additional Protections for Children's Personal Information

Increasing Costs of Non-Compliance

- **In Regulatory Context:**
  - Huge Financial Penalties; Criminal Penalties
  - Prohibitions on Processing Personal Data Usage
  - Prohibitions on Cross-Border Transfers
- **In Litigation Context:**
  - Class Actions
  - Individual Actions
  - Potential for Joint and Several Liability
- **In Client Context:**
  - Breach of Contract Actions
  - False Claims Actions
  - Termination of Contract/Loss of Future Business
  - Suspension or Debarment
- **In Court of Public Opinion:**
  - Downturn in New Client Opportunities
  - Potential Employee Turnover
  - Damaged Public Perception

CCPA Example: Potential Costs of Non-Compliance

- **Regulatory Fines**
  - $2500 per Unintentional Violation
  - $7500 per Intentional Violation
- **Private Right of Action for Data Breaches**
  - $100-$750 per Incident, per Consumer, or Actual Damages, If Higher
  - No Limit on Number of Private Actions
  - *No Actual Harm Required*
  - Actions can be Aggregated into a Class Action
  - Plaintiff's Lawyers Will Seek to Tack on Additional Penalties Under CA Unfair Competition Law
- **Damages Will Quickly Rise to the Level of Millions of Dollars**
  - For Example, Data Breach of 15,000 People Would Result in at Least $1.5 Million in Damages

EU General Data Protection Regulation Example: Potential Costs of Non-Compliance

42

- Regulatory Fines of Up to 20 Million Euros or 4% of Worldwide Annual Revenues
- Potential Criminal Sanctions, Including Imprisonment, Under Member State Laws
- Restrictions and Prohibitions on Data Processing and Transfer
- Individual and Collective Actions by Data Subjects (With Joint and Several Liability)

Overall Costs of a Data Breach Will Continue to Increase

- Costs Continue to Increase (up 12% from 2014)
- Average Cost Globally: $3.92 million
- **Average U.S. Cost: $8.19 million**
- Lost Business Constitutes Greatest Loss ($1.42 million)
  - 2019 Verizon Study Noted 69% of Survey Respondents Would Avoid a Company With a Data Breach (Verizon 2019 Data Breach Investigations Report)

Ponemon Cost of a Data Breach Report (2019) (sponsored by IBM Security)

Regulators Will Continue to Impose Increasingly High Numbers for Egregious Privacy Violations

- FTC: **$5 Billion** Penalty (Facebook)
- FTC, Consumer Financial Protection Board, States: **$575 Million** (Equifax)
- Nationwide Action: **$148 Million** (Uber)
- Multi-State Action: **$18.5 Million** (Target)
- ICO (UK): **€183 Million** (British Airways)
- ICO (UK): **€99 Million** (Marriott International)
- CNIL (France): **€50 Million** (Google)
- Multi-State Action: **$10 Million** (Premera Blue Cross)
- California: **$8.5 Million** (Wells Fargo)
- California: **$8 Million** (Comcast)
- California: **$3.4 Million** in Civil Penalties and Fees + **$25 Million** (customer refund) (Aaron's)

Privacy Class Action Litigation Will Continue to Proliferate

- *"The growing legislative trend to protect individual privacy and personal data…has brought a corresponding increase in class litigation.* ***Thousands*** *of class actions are filed each year under various privacy-related statutes, many of which provide for damages regardless of whether a claimant can demonstrate actual harm or injury as a result of the statutory violation."*
  -Jackson Lewis 2019 Class Action Trends Report

- *"As we move into a new decade, it has become clear that data breach litigation is here to stay."*
  -Data Privacy Monitor

Companies Will Continue to View Data Privacy and Protection as a Top Risk

- 2019 Gartner Emerging Risks Monitor Report: **Rapidly Accelerating Privacy Regulations and Associated Regulatory Burdens are *the* Top Emerging Risk**
  - Gartner Predicts That by 2021, 60% of All Large Organizations Will Have a Privacy Management Program Fully Integrated Into the Business, Which is Up From 10% in 2010 (Gartner for Legal and Compliance Leaders Working With GDPR: How Legal and Compliance Leaders Can Improve Data Protection (2019))
- 2019 Travelers Risk Index (Business Leaders of All Sizes of Businesses): **Cyber Risks are *the* Top Concern**
- 2019 KPMG Chief Compliance Officer Survey: **Privacy Listed as a *Top Five* Regulatory and Compliance Obligation of Focus**


402

Privacy Will Continue to Keep In-House Counsel Up at Night

- *"The steady stream of data security incidents making news headlines is a constant reminder of the potential risks that virtually every company currently faces. Just five or ten years ago, few in-house practitioners would have identified cybersecurity as their foremost concern.* ***Fast forward to 2018, and cybersecurity is a top-of-mind concern for a majority of general counsel."***

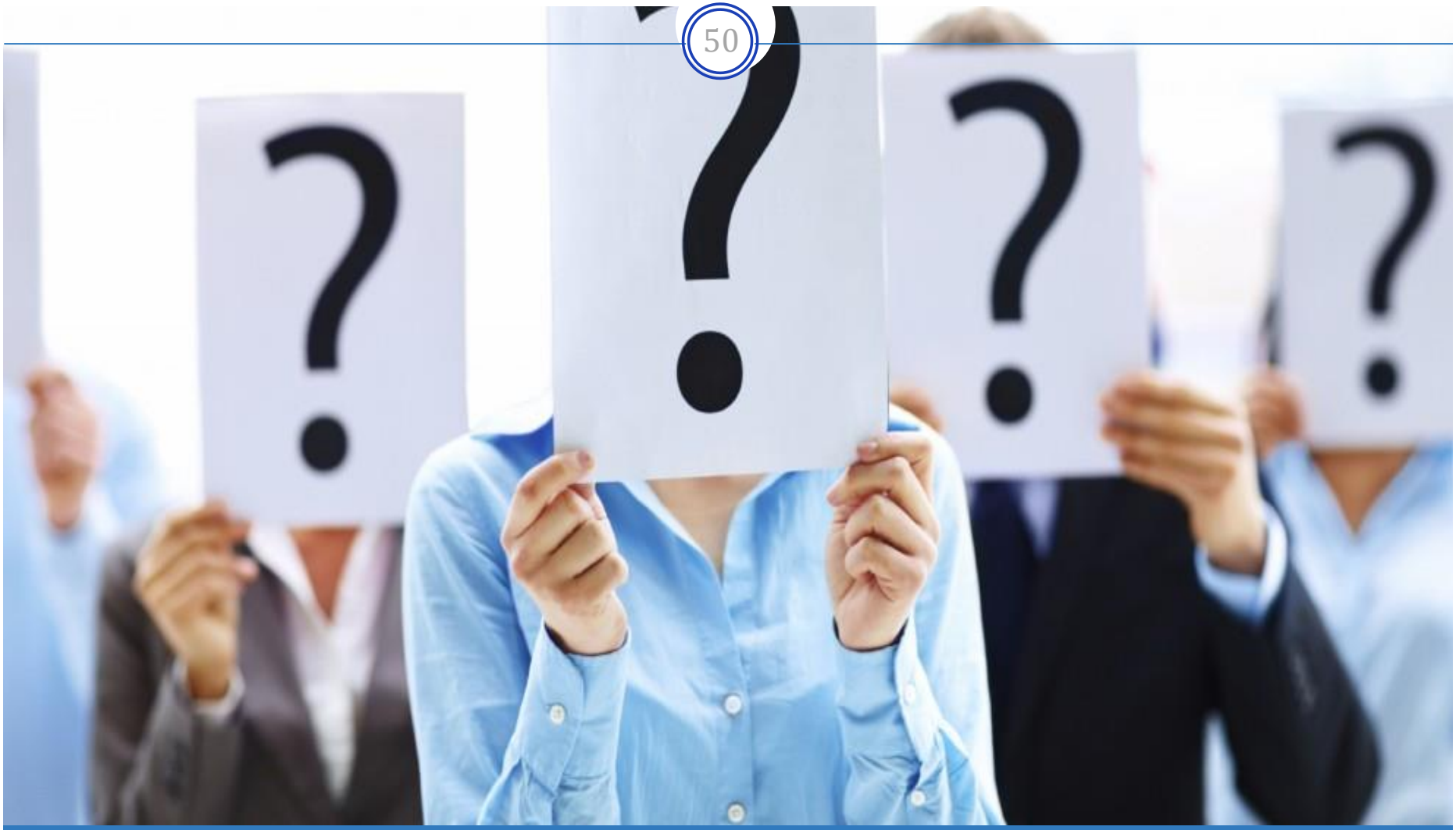
- *"****In this digital age where information has no borders, virtually every company has to worry about privacy****….The GC Up-at-Night research aims to understand how organizations are navigating in a fragmented global regulatory environment. This struggle is perhaps no more difficult than in the areas of privacy and security, where unsettled law, shifting norms, and rapidly changing technology multiply the challenges."*

-2018 ALM Intelligence/Morrison & Foerster General Counsel Up-at-Night Report

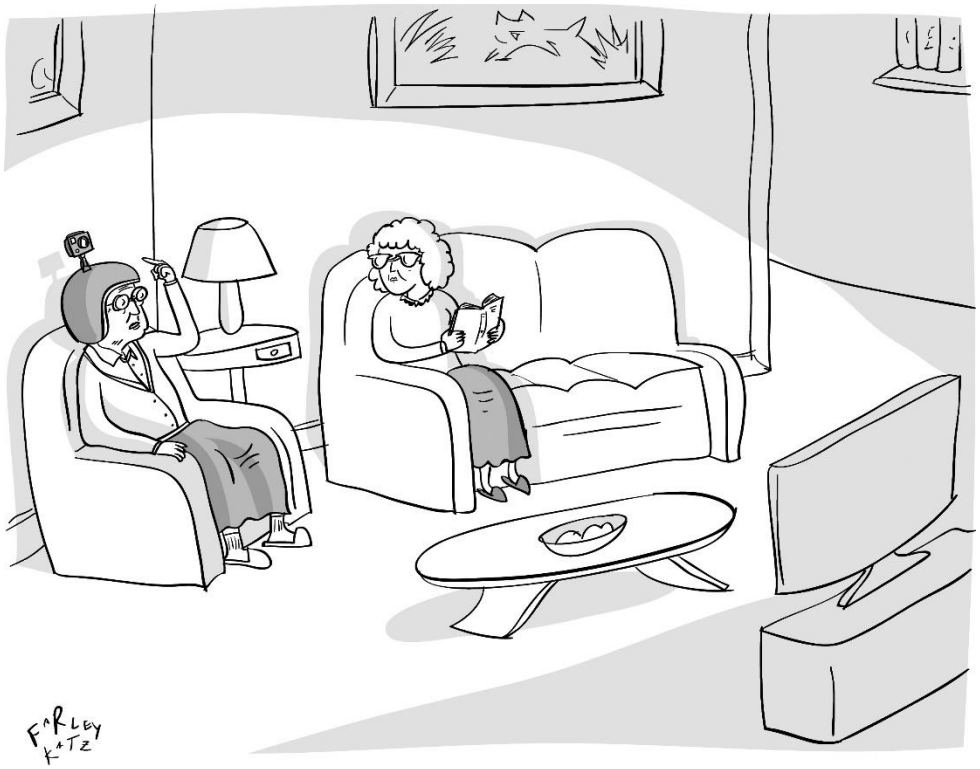
Privacy Will Continue to Keep In-House Counsel Up at Night

- *"In 2019, CLOs have their eyes on data.* ***Data breaches, regulatory changes, and information privacy top the list of concerns for CLOs in 2019.*** *With new regulations like GDPR governing data sharing and storage, it is foreseeable that a majority (68 percent) of respondents to this year's survey say they are very or extremely concerned with data breaches and the protection of corporate data, followed by 66 percent who cited regulatory or governmental changes as highly important. Information privacy (65 percent) rounds out CLOs' top three concerns in 2019."*

  -2019 American Corporate Counsel Chief Legal Officer Survey



Stay Well and Happy until We Meet Again



"I've got the whole night on GoPro in case we want to relive the excitement later."