WINSTON & STRAWN LLP

WEBINAR

Traversing the Employee-Monitoring Tightrope: Balancing Conflicting Responsibilities and Risks

JULY 30, 2020

SPEAKERS

AVIVA GRUMET-MORRIS
PARTNER

agmorris@winston.com

ALESSANDRA SWANSON
PARTNER

aswanson@winston.com

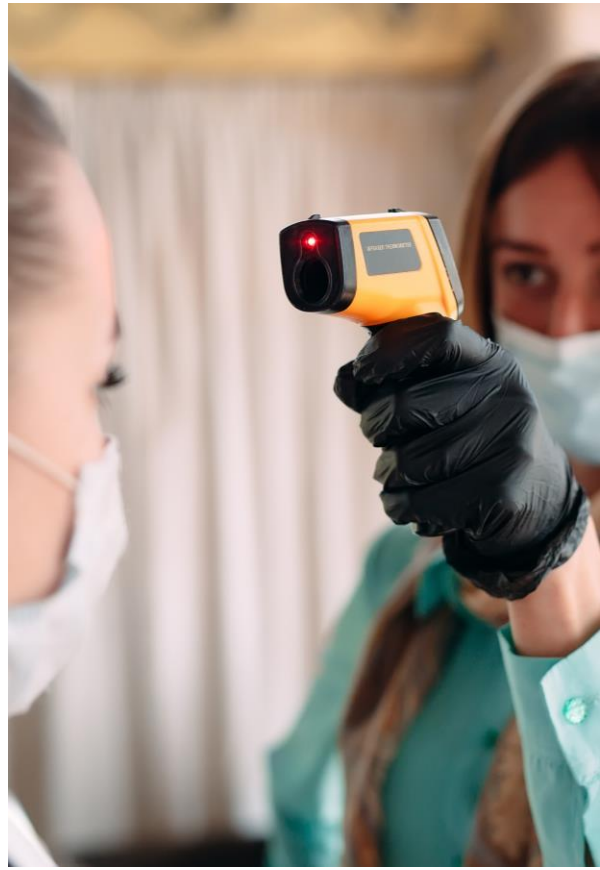
RECOVERY THREAT SCENARIOS

Employee-Monitoring Scenario

WINSTON & STRAWN LLP

What is EmployeeTemp?

- Scans employee's facial geometry
- Confirms employee's identity and
- Records employee's temperature
- EmployeeTemp sensors conduct biometric scans and temperature checks.



EmployeeTemp App

- Employee scans face
- App saves and stores biometric template
- On-site sensors match real-time facial scans to stored biometric templates to verify employee identity
- App asks employees questions

EmployeeTemp App Questions

Asks general medical history

Asks whether the employee or any member of his or her family currently

- have or in the past have had COVID-19
- are currently exhibiting COVID-19 symptoms, or
- have specific underlying medical conditions

Links to medical documentation from prior FMLA or other medical leaves of absence

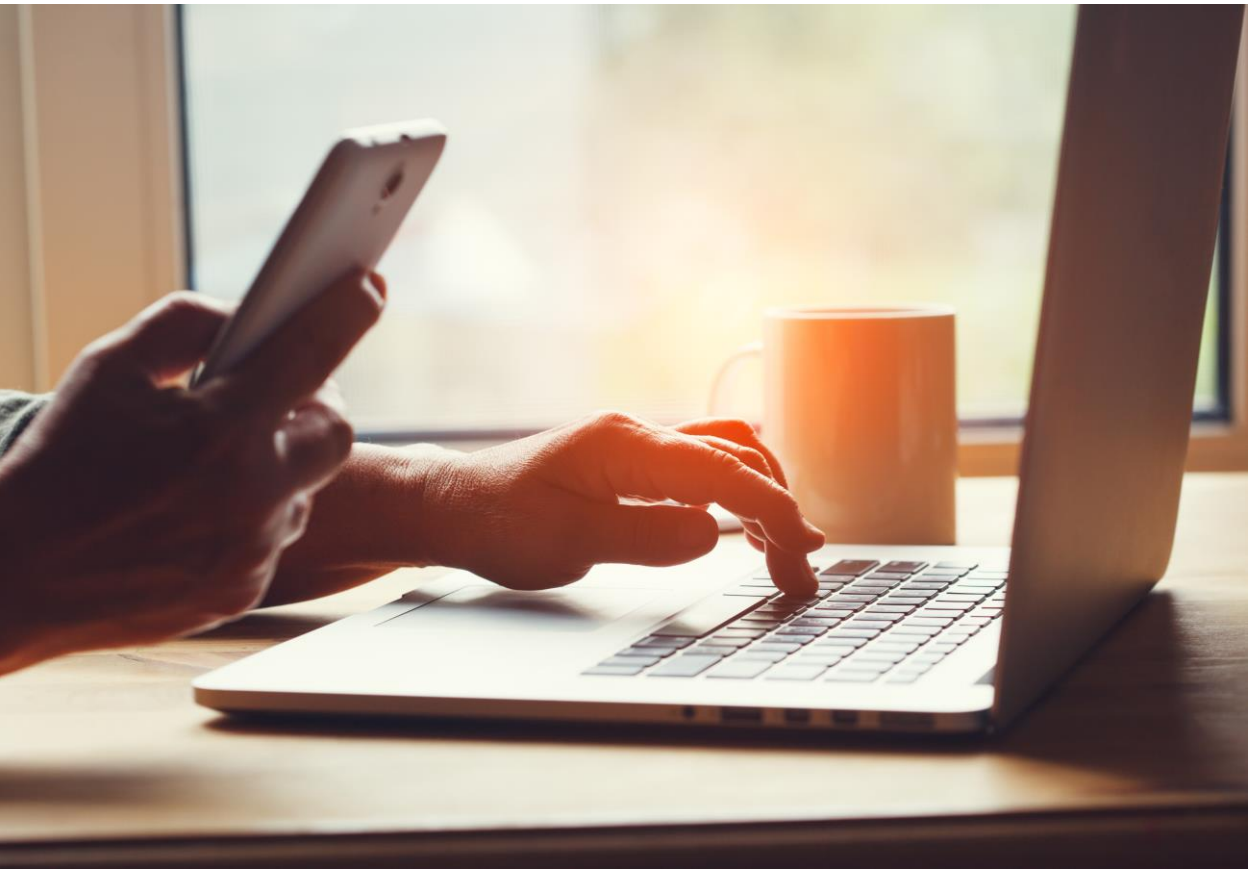
EmployeeTemp Online Platform

- Identity of entering employees
- Temperatures
- Personal and family medical histories
- Health-related documentation
- EmployeeTemp data can be downloaded to create reports

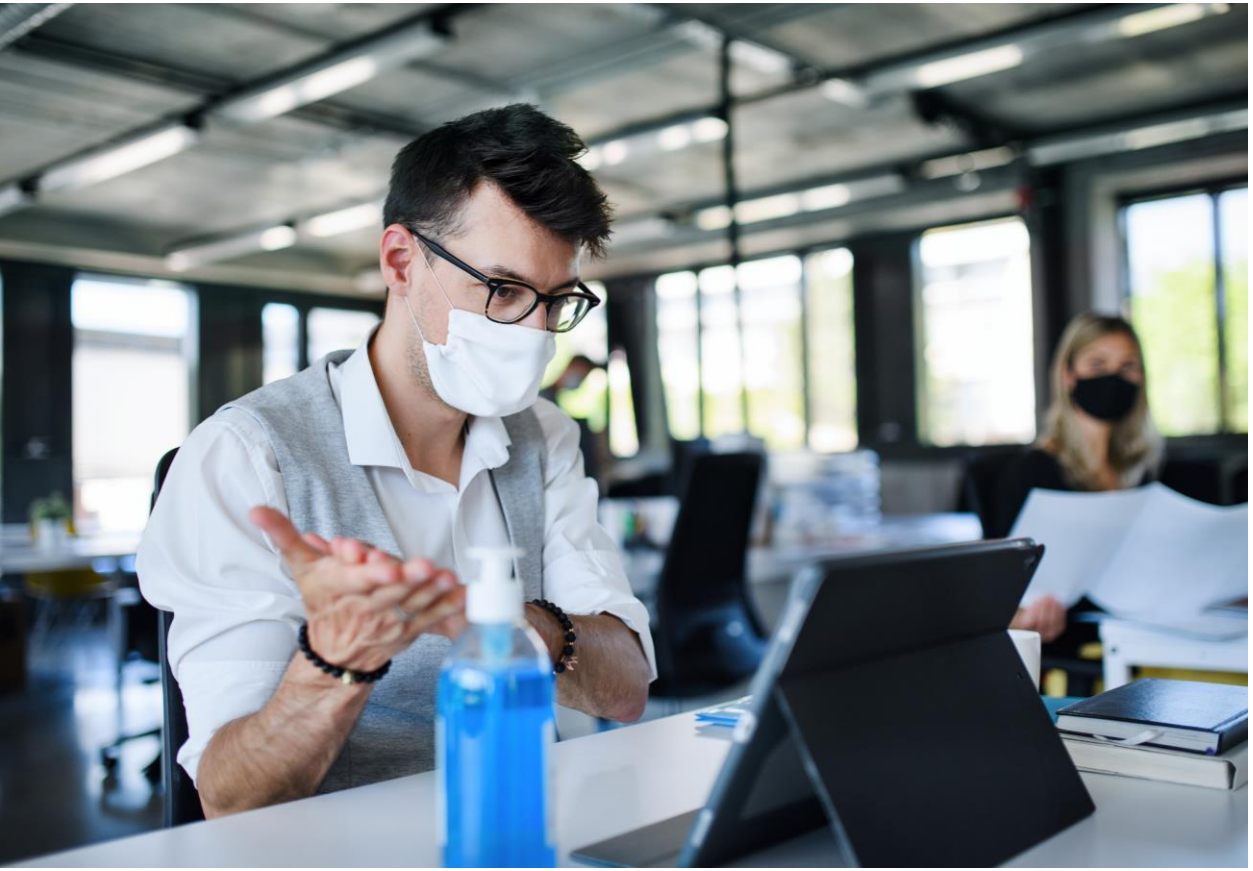
GenericCo Announces

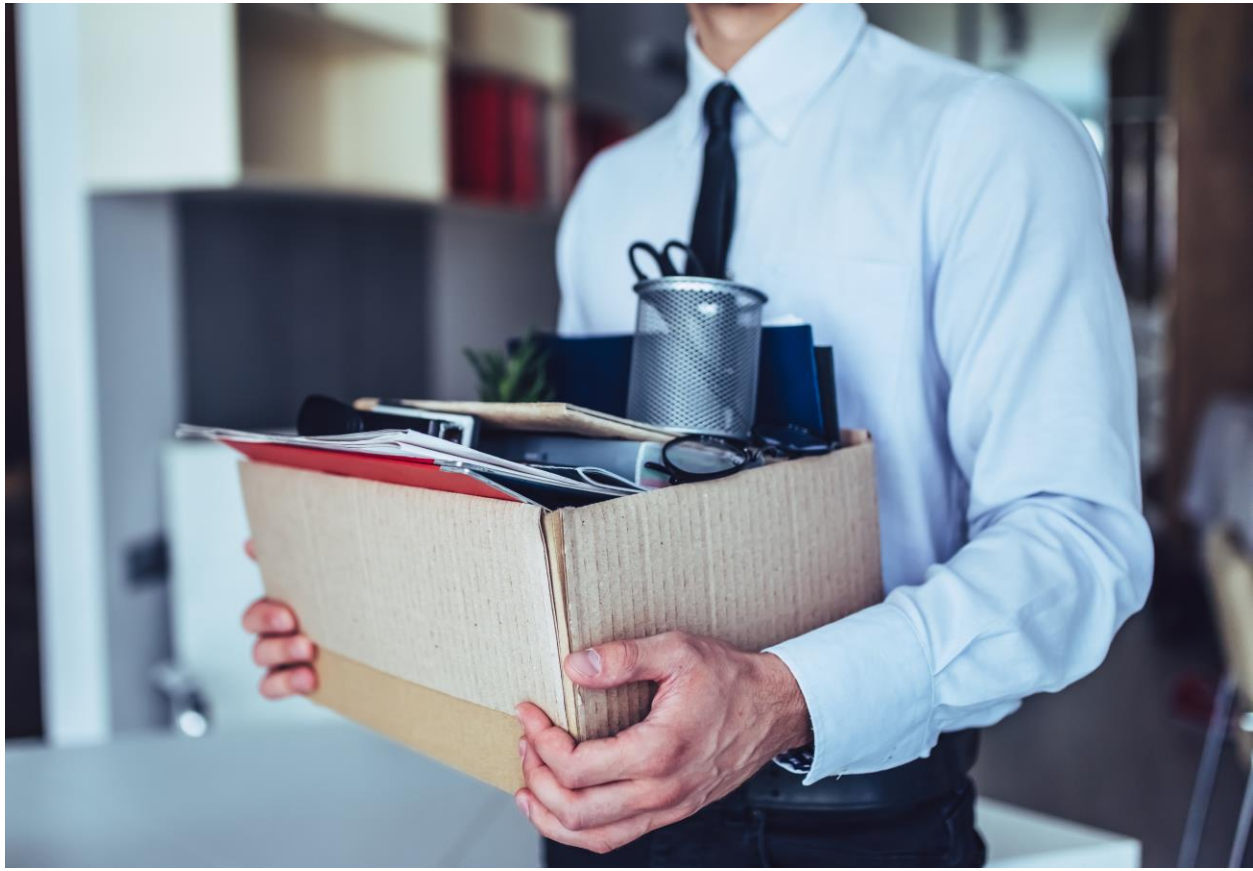
Employees with COVID-19 Symptoms	Will be sent home for 14 days	
Positive COVID-19 Diagnosis	Means “high risk” employees are sent home for 14 days	
“High Risk” Employees	• Pregnant • 65 years old or more	• Have underlying medical conditions • Have family members with underlying medical conditions
Access to EmployeeTemp	All HR members and upper level management have access to EmployeeTemp data and downloaded reports	

Jack Tired



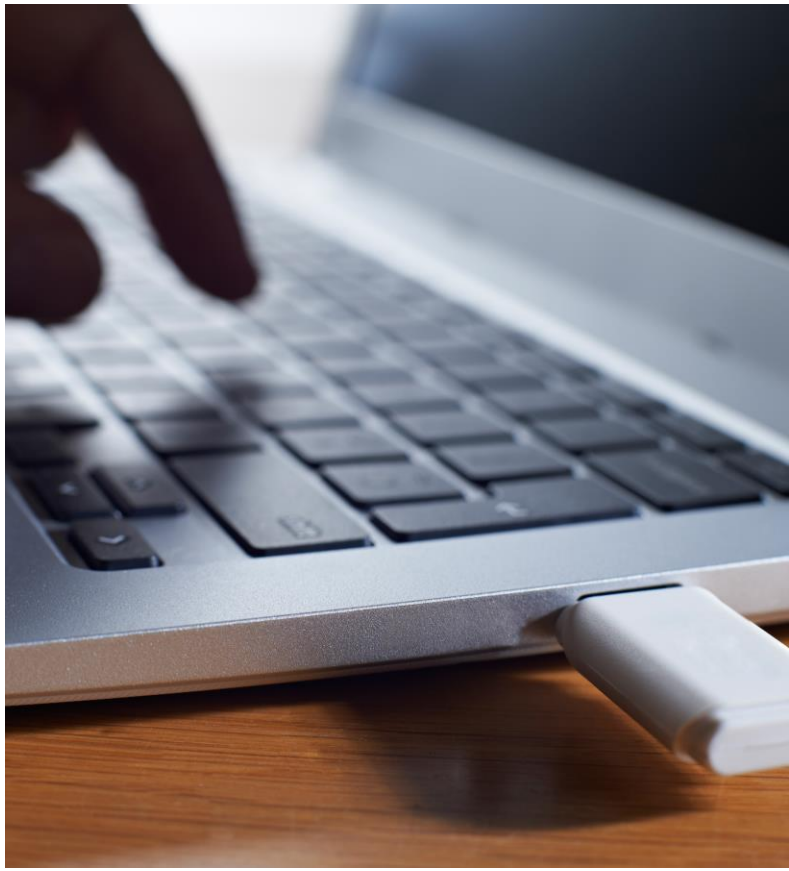
- HR employee working from home
- Clicks on email link in email while distracted
- Enters username and password
- Later establishes administrator account for EmployeeTemp portal





Security Breach

- FBI discloses data security breach
  - Sensitive information about employees accessed and put on dark web, including:
    - Social security numbers
    - Passport numbers
    - Driver's license numbers
    - Health-related data



GenericCo's Data Security Breach Response

- Engages legal counsel
- Retains forensics vendor to investigate
- Identifies cause and duration of breach
- Provides written notification of incident to:
  - Employees
  - State Attorneys General

Legal and Financial Impact

- Millions of dollars spent on expert investigation, remediation, legal compliance work, notification and credit monitoring services
- California employee lawsuit – CCPA violations - $2.25 million in statutory damages
- Illinois employee lawsuit – BIPA violations - $5 million in statutory damages
- Additional data security class actions
- State Attorneys General investigations
- EEOC charges of discrimination

What did GenericCo do right in the scenario?

A	Implemented a health screening program to address COVID-19 in the workplace
B	Refrained from disclosing how the biometric and personal information was being collected and stored – employees are being inundated with too much information these days
C	Took immediate action upon learning of the data breach – retained counsel, retained forensic vendor, complied with state breach notification laws
D	Immediately terminated employees who refused to provide biometric scans and/or answer questions – GenericCo doesn't need troublemakers in these uncertain times
E	Both A and C
F	All of the above
G	None of the above

A	Implemented a health screening program to address COVID-19 in the workplace
B	Refrained from disclosing how the biometric and personal information was being collected and stored – employees are being inundated with too much information these days
C	Took immediate action upon learning of the data breach – retained counsel, retained forensic vendor, complied with state breach notification laws
D	Immediately terminated employees who refused to provide biometric scans and/or answer questions – GenericCo doesn't need troublemakers in these uncertain times
E	Both A and C
F	All of the above
G	None of the above

What did GenericCo do right in the scenario?

- GenericCo was right to implement employee health screenings
- Nothing inherently wrong with virtual health screening programs
- GenericCo had the right response to the data security breach
- GenericCo correctly sent home employees with symptoms of COVID-19

What did GenericCo do wrong in the scenario?

A	Failed to provide necessary disclosures and obtain necessary consents from employees for the collection and storing of biometric data and personal information
B	Required employees to answer questions in the EmployeeTemp App beyond what is permitted under the ADA and GINA
C	Failed to implement the necessary controls to ensure the confidentiality of medical information, including limiting access to few individuals and encrypting data
D	Forced older, pregnant, and/or disabled workers to take involuntary leaves of absence to keep them and their family members safe
E	Both A and C
F	All of the above
G	None of the above

A	Failed to provide necessary disclosures and obtain necessary consents from employees for the collection and storing of biometric data and personal information
B	Required employees to answer questions in the EmployeeTemp App beyond what is permitted under the ADA and GINA
C	Failed to implement the necessary controls to ensure the confidentiality of medical information, including limiting access to few individuals and encrypting data
D	Forced older, pregnant, and/or disabled workers to take involuntary leaves of absence to keep them and their family members safe
E	Both A and C
F	All of the above
G	None of the above

WINSTON & STRAWN LLP

Legal Issues

Disability-Related Inquiries and Medical Examinations

- Americans with Disabilities Act (ADA) regulates
  - disability-related inquiries and
  - medical examinations
- Direct Threat: a significant risk of substantial harm to the health or safety of employees that cannot be eliminated or reduced by reasonable accommodation
- EEOC: COVID-19 meets the direct threat standard
  - But: must be related to keeping the virus out of the workplace

EmployeeTemp App Questions – Lawful or Prohibited?

✓ Questions about COVID-19 symptoms

✓ Taking employee body temperature

✓ Asking about current COVID-19 diagnosis or pending test results

× Asking about a having COVID-19 in the past

× Asking about family member COVID-19 diagnoses or symptoms

× Asking about employee general medical histories or linking to historical medical documentation

× Asking about employee or family member medical conditions associated with COVID-19 complications

GenericCo Runs Afoul of Biometrics Laws

- Biometric data collection is not prohibited
- GenericCo failed to consider in which jurisdictions will the information be collected
  - IL, WA, CA and TX have biometric privacy laws and many others have specific data protection requirements or consider biometric data to be “triggering” under breach notification laws
  - In this scenario, GenericCo did not consider the Illinois Biometric Information Privacy Act (BIPA) which contains strict notice and consent requirements, and can introduce high statutory damages merely for failing to provide these notices
- Other items to consider:
  - Individuals outside of IL may be able to bring claims under BIPA
  - A breach of biometric information can trigger statutory fines under the California Consumer Privacy Act (CCPA) and data breach lawsuits in other states

Confidentiality Under the ADA

ADA requires medical information

- be kept confidential
- be collected and maintained on separate forms and in separate files
- be treated as confidential medical records

Employers must restrict access to confidential medical information, including:

- information obtained through disability-related inquiries or medical examinations
- “genetic information” under GINA.

How did GenericCo Fail to Maintain Confidentiality?

× Too many people have access to employee confidential medical information
  - Mr. Reckless
  - All members of Human Resources
  - Upper level management

✓ Better Plan: Limit access to confidential medical information to a few COVID-19 point people

× Downloading and circulating confidential medical information

✓ Better Plan: Do you need to download and circulate confidential medical information? If so, who needs to see that data?

Employee Data Security Issues

- Right now, we are all “Jack Tired” in some respect
  - The combination of pandemic-related stress, lack of childcare and potentially less-than-ideal home working conditions can create situations where employees are more distracted
- What went wrong at GenericCo?
  - Jack clicked on a “phishing” email that enabled a bad actor to access his email inbox
  - GenericCo employees were encouraged to use their log-on credentials to access multiple platforms
  - A significant amount of sensitive employee personal information was stored in Jack’s email
  - Data was exfiltrated without detection

How did GenericCo err in implementing the EmployeeTemp product?

× Firing employees for refusing to answer EmployeeTemp app questions

  - Why did employee refuse to download the app or answer questions?
  - Were they remote workers?
  - Is there another legitimate reason for their refusal?

- Involuntary leave of absence for employees with family members having an underlying medical condition is
  - discrimination based on relationship or association under the ADA
  - discrimination based on genetic information under GINA
- Involuntary leave of absence for employees with underlying medical conditions solely because of those conditions is disability discrimination under the ADA

GenericCo Suffers a Security Breach…

- Once GenericCo confirmed that a breach had occurred, it was required to undertake the process of notification
  - This involves hiring legal counsel to assess 50 different state laws (each have different definitions of what constitutes “personal information” and “security breach”)
  - Forensic vendors work to contain and remediate the breach, communicate and negotiate with bad actors, attempt to get data off of the dark web (which doesn’t always work)
  - Notification and credit monitoring is usually provided through a third-party vendor
  - Sometimes crisis communications teams are leveraged to help with messaging, especially once data is exposed
- As a practical matter, this is around-the-clock work, expensive work

… and Creates The “Perfect” Storm for Litigation

- Aggressive Plaintiffs’ Bar
  - There is easy access to information about security breaches via state Attorney General websites
- Uncapped Statutory Damages
  - BIPA and CCPA are strict liability laws that lead to “bet the business” class action damages calculations
- Vague and Ambiguous Statutes
  - BIPA case law has barely evolved beyond the lack of notice and consent, while CCPA lacks any meaningful definition of “reasonable security procedures and practices”
- Ever Changing Regulatory Landscape
  - While we focused on BIPA and CCPA today, at any given time there are copycat laws proposed in at least ten or more states

GenericCo Faces Dozens of Charges of Discrimination

- EEOC enforces ADA, Title VII, GINA, and the ADEA
- Employees can file charges of discrimination
- EEOC investigates allegations
  - No reasonable cause to believe discrimination occurred – Dismissal and Notice of Rights (employee can file lawsuit)
  - Reasonable cause to believe discrimination occurred – Letter of Determination and effort to conciliate (if no resolution, either EEOC or employee can file lawsuit)
- Once the EEOC is involved, the agency does not have to stop investigation even with private settlement of the dispute

WINSTON & STRAWN LLP

Don’t Be the Next GenericCo

Don’t Be the Next GenericCo

1. Involve subject matter experts regarding health screening programs
   - HR
   - Legal / Regulatory / Compliance
     - privacy/data security, employment, commercial contracting, employee benefits
   - IT / Cybersecurity
   - Operations
2. Know what disability-related information can be requested from employees
3. Understand what medical information is being collected and how that information will be maintained to ensure confidentiality
4. Avoid forcing employees to take involuntary leaves of absence merely because they or their family members are part of a “vulnerable population”

Don’t Be the Next GenericCo

5. Make sure you identify and weigh benefits and risks of virtual health screening programs
6. Understand the range of state privacy laws, including consent and notification requirements
7. Know what states have the highest risks exist and determine whether to treat that jurisdiction differently
8. Have a process in place to identify data security breaches and quantify exposure
9. Understand who is hosting data
   - If it is a vendor, understand the contractual provisions related to indemnification, data collection, and data dissemination
   - If the hosted data is sensitive, ensure sufficient data security measures
10. Establish and enforce good practices and policies regarding
    - collection and dissemination of information
    - handling of biometric data

WINSTON & STRAWN LLP

Questions?