WINSTON & STRAWN LLP

Top 10 Privacy Changes in 2019 & Navigating Privacy Compliance in 2020

January 21, 2020

Today’s Webinar Presenters

Sheryl Falk

Litigation
Houston
sfalk@winston.com

Alessandra Swanson

Corporate
Chicago
aswanson@winston.com

Sean Wieber

Litigation
Chicago
swieber@winston.com

Eric Shinabarger

Litigation
Chicago
eshinabarger@winston.com

WINSTON & STRAWN LLP

The Top 10 Privacy Changes in 2019

Roadmap: Where We Are Headed Today

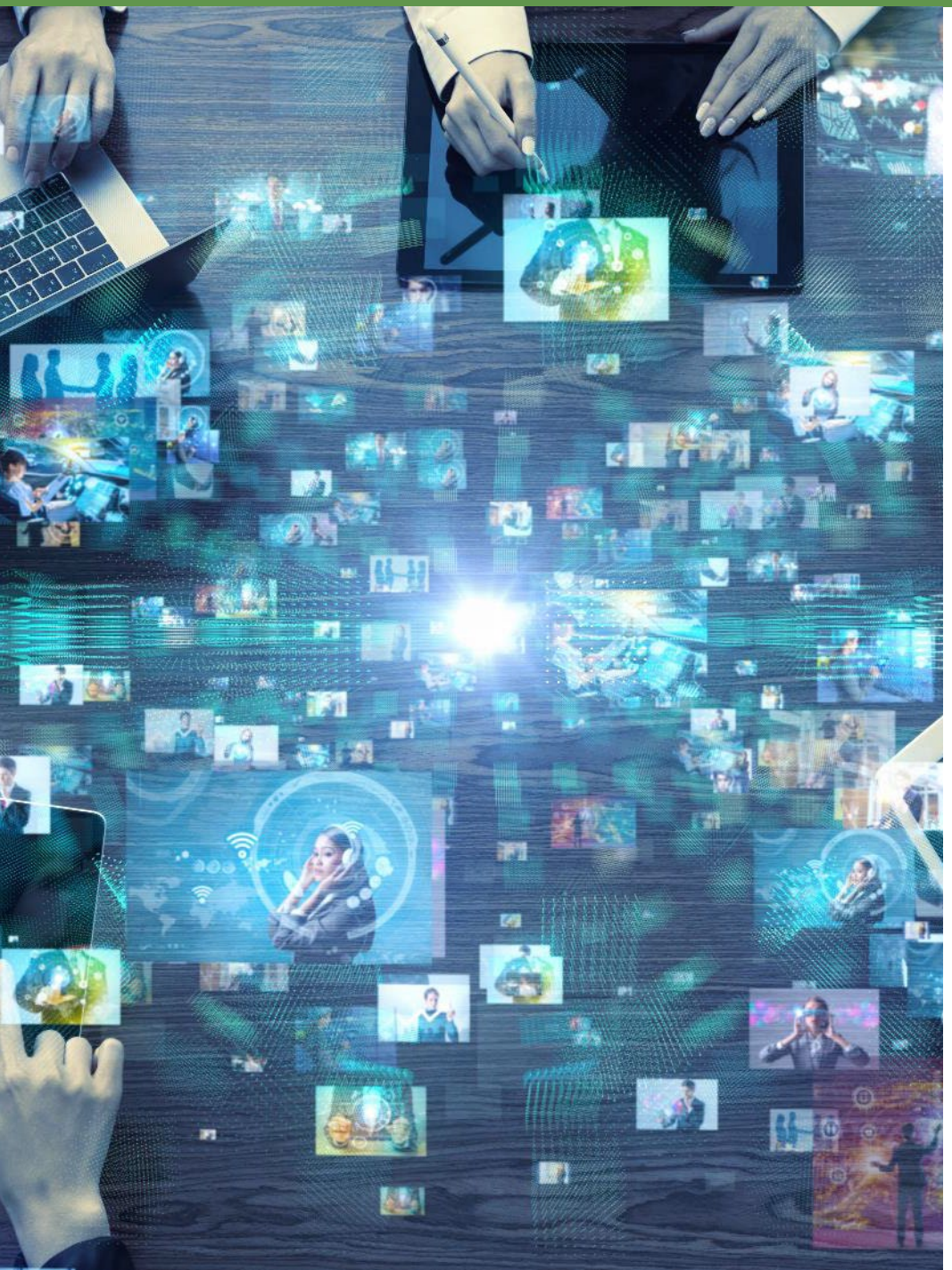
1. CCPA – Amendments/Guidance
2. Other states took up privacy legislation
3. New AI law – Illinois
4. Biometric regulation and litigation
5. IOT laws in effect (California/Oregon) and “reasonable security”
6. NY SHIELD Act
7. FTC fines – COPPA settlement/Facebook
8. TCPA update
9. GDPR enforcement
10. New international privacy laws

1 The California Consumer Privacy Act – Now in Effect

- In effect as of January 1, 2020, with enforcement beginning in July 2020
- Draft regulations released in October 2019, with a final version expected in spring 2020
- Final amendments enacted in October 2019
- However, additional changes may still come, including:
  - Additional amendments, and
  - A second ballot initiative

2 States Considering Privacy Legislation

- Several states have enacted more limited legislation governing online privacy practices (Nevada, Maine, several others pending)
- Others (e.g., Massachusetts and New York) would go beyond CCPA
- Four states have proposed CCPA copycats thus far in 2020
  - Includes Washington, which re-introduced a CCPA copycat in January 2020



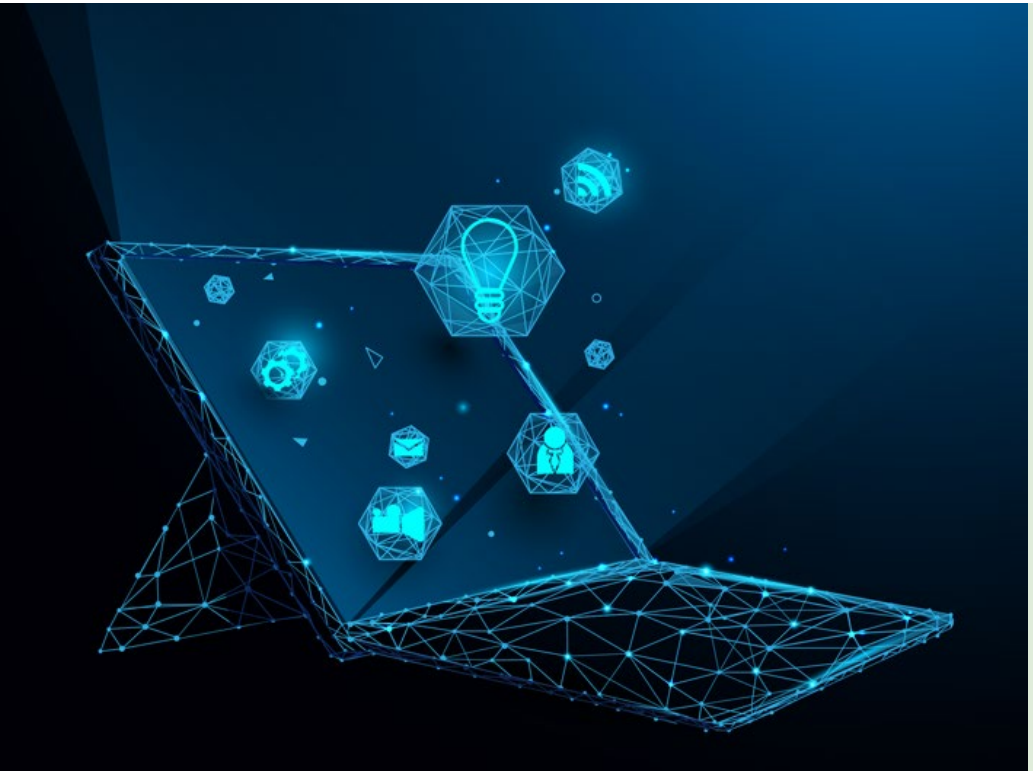
3 Illinois AI Video Interview Act

- Applies to every employer seeking to fill a position in Illinois:
  - **TRANSPARENCY**: Notify each applicant before the interview that AI may be used to analyze the applicant's video interview and consider the applicant's fitness for the position.
  - **EXPLAINABILITY**: Provide each applicant with information before the interview explaining how the AI works and what general types of characteristics it uses to evaluate applicants.
  - **CONSENT**: Obtain, prior to interview, consent from applicant to be evaluated by the AI program.
  - **CONFIDENTIALITY**: Must not share video except with those needed to evaluate applicant.
  - **DESTROY COPIES**: Upon request, must destroy all copies 30 days after request.
- Currently there are no penalties for lack of enforcement.

4 Biometric Regulation & Litigation

- Additional case law in Illinois state courts continues to help define the law
- Facebook continues to defend a massive BIPA class action in the 9th Circuit
- States continue to propose BIPA copycats, but IL, TX, and WA remain the only states with general biometric-specific laws
  - SC's BIPA copycat includes a private right of action and some of the rights found in the CCPA
  - WA may update and strengthen its current biometric law by further restricting the use of biometric data and providing CCPA rights

5 IoT Laws – California and Oregon



- Laws regulating "connected devices" went into effect on January 1st in both California and Oregon
  - Essentially a de facto national law given the inability to segment products intended for California or Oregon
- "Connected devices" defined broadly
- Manufacturers of connected devices required to use non-unique passwords and implement "reasonable" security features

6 NY SHIELD Law

- The SHIELD act requires employers in possession of NY resident's private information to "develop, implement, and maintain reasonable safeguards to protect the security, confidentiality, and integrity of the private information."
  - Some exceptions for small businesses
  - Similar to the written information security program requirements under MA law
- Expands breach notification requirements
- Goes into effect: March 21, 2020

7 Federal Regulators Stepping Up Enforcement

Unnamed U.S. Energy Firm	$10 million fine by NERC for violating 127 CIP standards
Facebook	$5 billion fine and mandatory oversight
Equifax	$275 million fine for improperly protecting consumer data, leading to the largest data breach in history
UnrollMe	Settling allegations that the company misled consumers. No penalty, but required remediation of misleading statements
DLink	Settling allegations that the company overstated its products' security capabilities. Required comprehensive software security program

8 TCPA Update

- ATDS – Courts continue to weigh in on the types of devices that are considered an “automatic telephone dialing system”
- The debt-collection exemption called into question
- Standing – can a plaintiff establish a real and tangible harm, such as where a plaintiff receives a single call or text?
- Personal liability for officers and directors

9 GDPR Enforcement

- Enforcement began in May 2018
  - Roughly €360 million in fines so far, most in 2019
- A few of the bigger fines:
  - **British Airways** – UK regulator fines British Airways €183 million for a breach affecting 500,000 customer records due to poor cybersecurity
  - **Google** – Fined €50 million by French regulator for lack of transparency
  - **Marriot** – UK regulator fines Marriott €99 million for a data breach affecting 30 million EU residents
- Multi-billion € fines **imminently expected** against large tech companies by the Irish regulator

10 New International Data Protection Laws

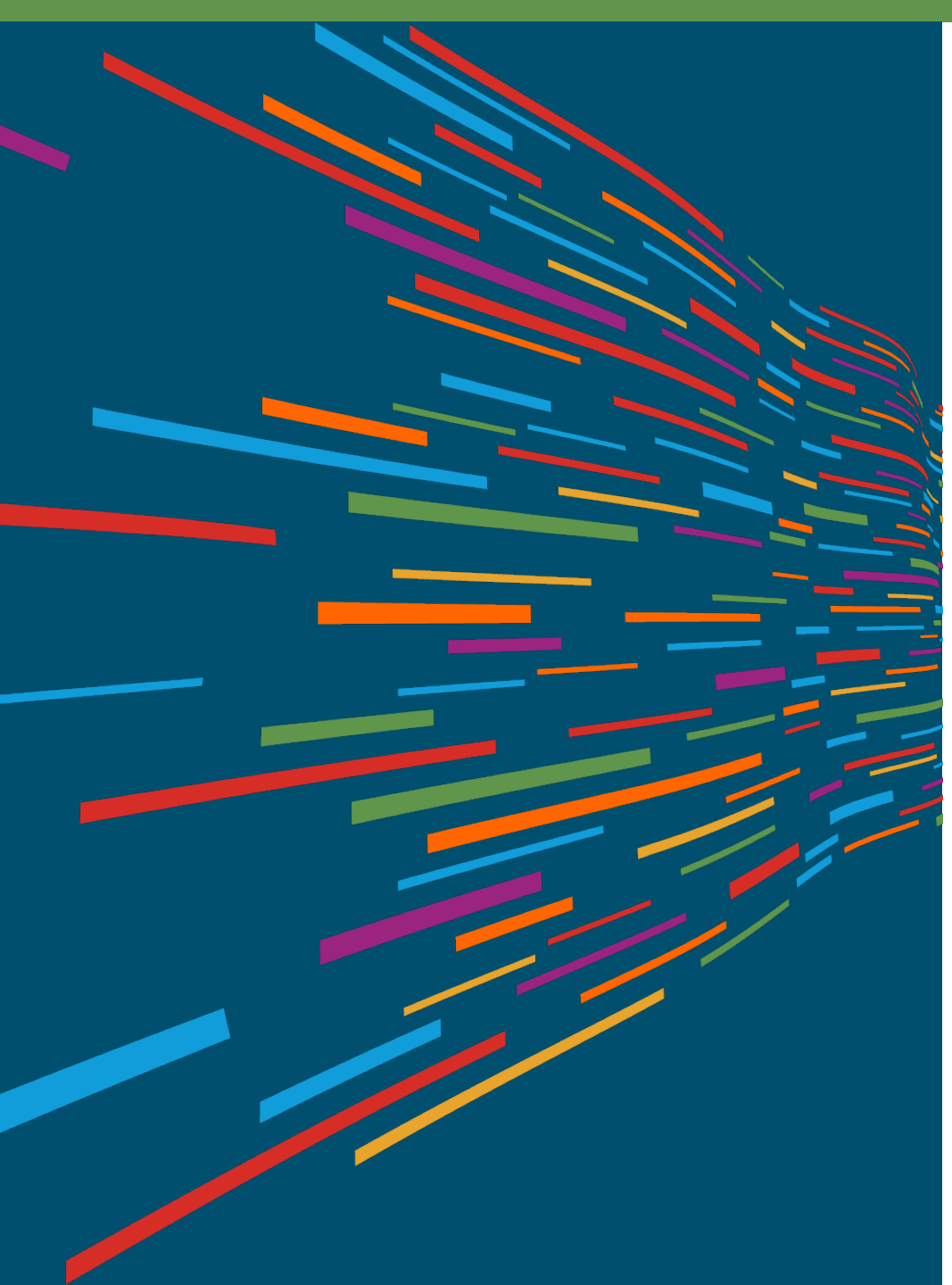
The challenge is how to keep up with emerging and conflicting data protection standards...

Brazil

Canada

China

Singapore



What We're Watching in 2020

- CCPA – Additional guidance/finalizing of rules/enforcement
- CCPA – private right of action
- California enforcement actions re: IOT
- FCC clarifications re: TCPA
- Class action data security litigation
- Additional emerging tech legislation
- Federal privacy legislation

Steps to Take Now

Make sure the C-Suite/Board are aware of the risks

Understand your data flow

- How does information flow through your company?
- Where does it come from, where is it stored, and where does it go?

Implement data minimization

- Do you need it?
- Can you get rid of it under a data retention policy?

Monitor developments in the law

- Understand the scope of your potential liability

Steps to Take Now

Assess data security

- Undergo an audit, certification, and/or penetration testing
- Implement additional established frameworks (e.g., NIST)
- Update breach response plan (!)
- Prepare for increase in litigation as well as the continued prevalence of ransomware attacks

Implement privacy and data security by design

- Involve the lawyers when designing products/services

Steps to Take Now

Review/update your policies and procedures

- Account for disclosure requirements
- Process for consumer requests
- Ensure your web page/statements are accurate!
- Monitor/train employees

Update your contracts

- GDPR/CCPA – specific contractual requirements
- Are you “selling” data?
- Talk to your vendors

Consider cyberinsurance

- The insurance industry is continuing to evaluate how it will handle privacy and data security liability

Thank You

Sheryl Falk

Litigation
Houston
sfalk@winston.com

Alessandra Swanson

Corporate
Chicago
aswanson@winston.com

Sean Wieber

Litigation
Chicago
swieber@winston.com

Eric Shinabarger

Litigation
Chicago
eshinabarger@winston.com