



YOUR DELAWARE ADVANTAGE

PRIVACY IN A PANDEMIC: Critical Legal Developments and Practical Guidance

Secure Delaware 2020

William R. Denny

October 27, 2020

Recent Privacy Trends and Practical Guidance

- Serious Privacy Impacts
- Comprehensive Privacy Laws
- Biometrics
- Geolocation and Contact Tracing
- Recommended Actions

New Threats to Privacy and Security

- Remote work
- New technology tools for communication
- New IT environments
- Use of unvetted personal devices and WiFi
- Stressed employees

Phishing Scams



4

- Cancel shipment due to coronavirus – details attached
- Corona is spinning out of control
- Feeling helpless against Corona
- Military source exposes shocking TRUTH about Coronavirus
- Get your coronavirus supplies while they last



Ransomware

- New variants of ransomware
- Exfiltrating data with a demand for further payment
- Blackbaud hack affected 3 million customers
- Significant risk of third-party vendors



Geolocation

- Online Fitness Tracker
Strava
- Mobile phone GPS
- Global “heatmap” showing
1 billion activities
- Danger of combining data
with other data

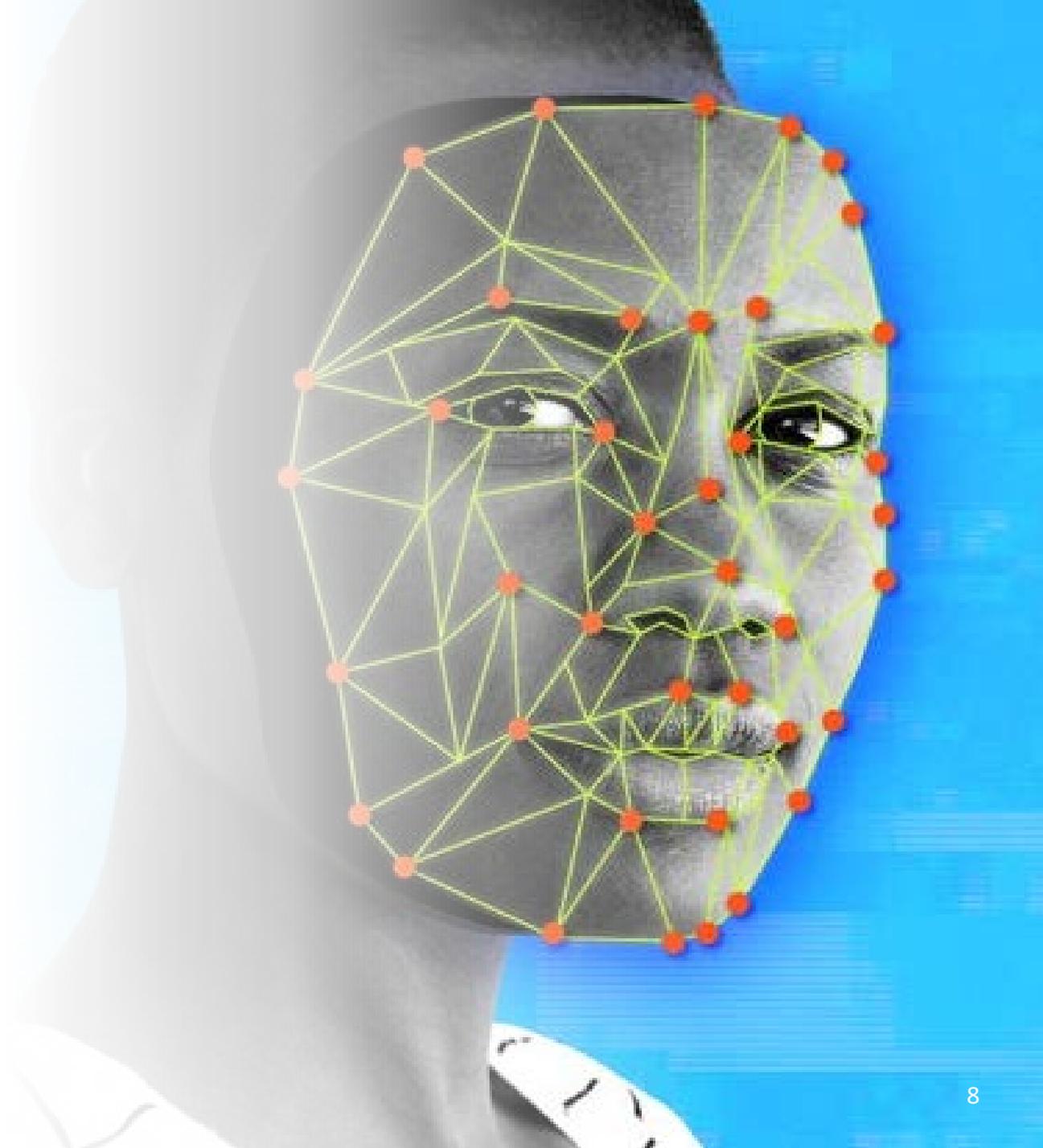


Social Engineering

- Twitter Hack
- Zoombombing

Biometrics

- Clearview.ai and facial recognition
- Database of billions of images
- Danger of abuse by law enforcement, private companies
- Lost its entire client list to hackers



Recommended Protective Measures

- Use VPN
- Multi-factor authentication
- Install security patches and upgrades
- Anti-virus and anti-malware software
- Replace legacy software
- Scan email
- Access control
- Policies for handling confidential information
- Strong passwords
- Training

Major Legislative Developments

- Since 2018, comprehensive consumer privacy laws introduced in at least 26 states and federal government
- California – CCPA, CPRA
- Illinois – Biometric Information Privacy Act
- International – Invalidation of Privacy Shield

California Consumer Privacy Act (CCPA)

- Effective January 1, 2020
- Comprehensive privacy law, broadly applicable to businesses regardless of location that collect or control personal information about California residents
- Substantial new rights for individuals
- Broad definitions
- Significant operational impacts
- Private right of action and high fines
- Effectively a floor for data rights across the country

Key components of CCPA

- Vastly expanded consumer rights
 - Right of Access
 - Right of Rectification
 - Right of Deletion
 - Right of Restriction
 - Right of Portability
 - Right of Opt-out of Sale
 - Right Against Automated Decision-making
 - Private right of action
- Notice at the point of collection
- Detailed notice requirements
- Risk assessments
- Website updates and consumer rights mechanisms
- Vendor contractual terms

California Privacy Rights Act (CPRA)

- Ballot initiative for November 2020, to be effective January 1, 2021.
- Replaces and expands CCPA
- New protections include:
 - New obligations regarding sensitive data
 - Sharing limitations
 - Enhanced protection for minors
 - Creation of California Privacy Protection Agency (CPPA)

Possible Federal Privacy Legislation

- All sides are pushing for a comprehensive national privacy framework.
- Latest bills:
 - Data Accountability and Transparency Act of 2020, introduced on June 18, 2020.
 - SAFE DATA Act
- Issues to resolve:
 - Preemption of state laws
 - Private right of action
 - Meeting adequacy requirements of GDPR
 - Enforcement agency

EU-US Privacy Shield Goes Down

- EU's top court decided *Shrems II* on July 16, 2020.
- Key data transfer mechanism used by thousands of U.S. companies
- GDPR prohibits transfer of data to countries lacking an “adequate level of protection” absent an approved mechanism.
- Current backup method, “Standard Contractual Clauses,” gets more complicated.

Geolocation and Contact Tracing

- Critical for containing COVID-19
 - But requires buy-in, affirmative consent
 - Subset of Personal Information
- Subject to multiple privacy laws
 - Illinois' Biometric Information Privacy Act (BIPA)
 - California Consumer Privacy Act (CCPA)
 - Health Insurance Portability and Accountability Act (HIPAA)
 - Numerous legislative proposals
 - Fourth amendment to U.S. Constitution
- In Delaware:
 - Prohibition against placing location tracker on motor vehicle without consent of owner.
 - Criminal offense to use geolocation data in connection with illegal dissemination of images.

Practical Guidance

- Understand applicable laws and regulations
- Conduct a risk assessment
- Implement reasonable security and privacy practices
- Prepare a written information security program
- Develop an incident response plan
- Train employees on security and privacy obligations
- Conduct risk assessment on third-party vendors
- Review insurance coverage for cyber-related incidents

Key Issues to Consider

- Data flows – what data are we generating?
- Do we have necessary consents to collect data?
- Are we collecting or using sensitive data categories?
- Can we de-identify the data?
- What are we doing with our data?
- What rights do we have in the data?
- What happens to data at the end of a relationship?
- Who are our customers and partners?

Contact Us

William R. Denny

Direct dial: (302) 984-6039

wdenny@potteranderson.com

Potter Anderson & Corroon LLP

1313 North Market Street

Wilmington, DE 19801

www.potteranderson.com