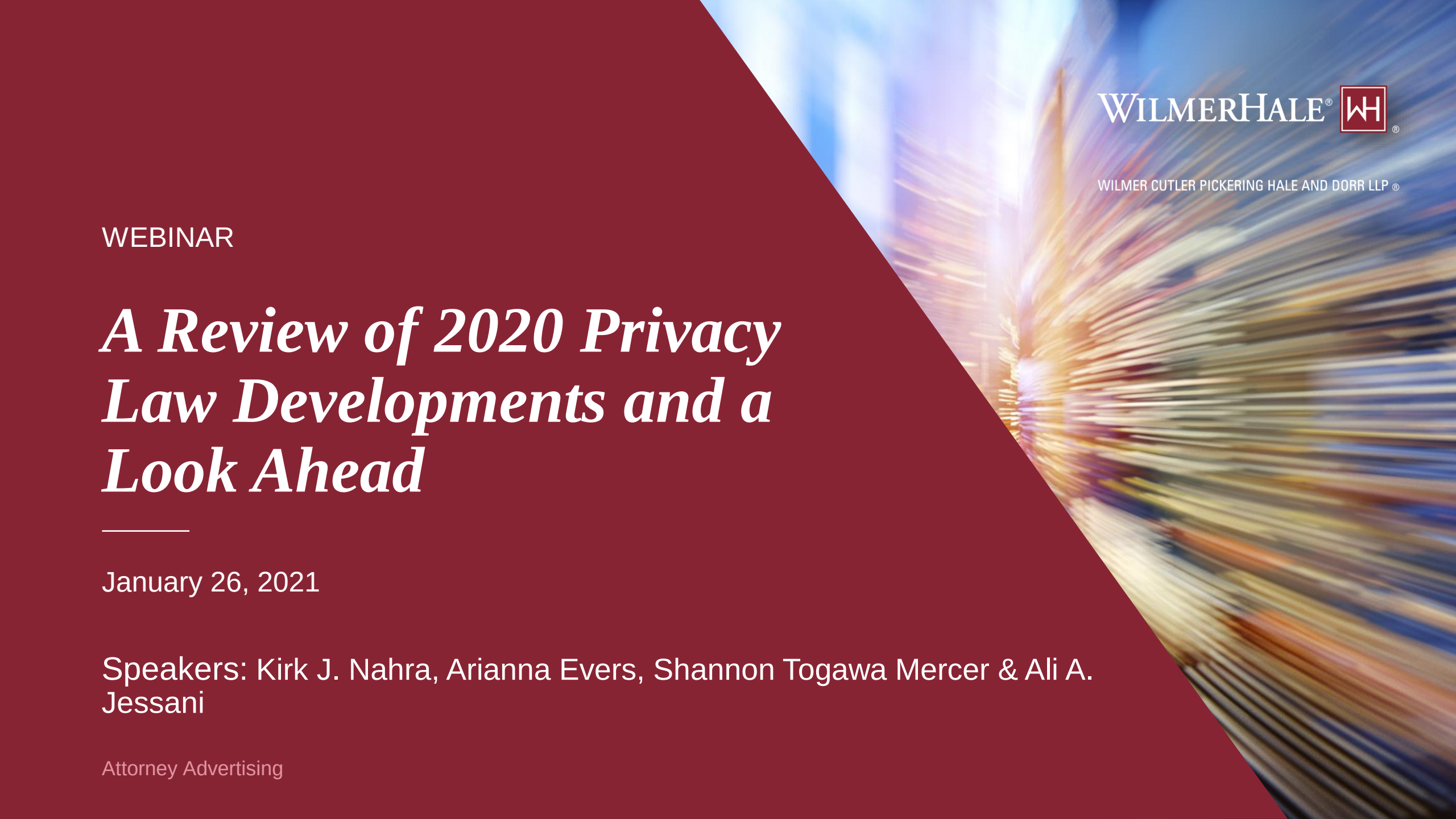


WILMERHALE®

WILMER CUTLER PICKERING HALE AND DORR LLP®

WEBINAR

A Review of 2020 Privacy Law Developments and a Look Ahead

January 26, 2021

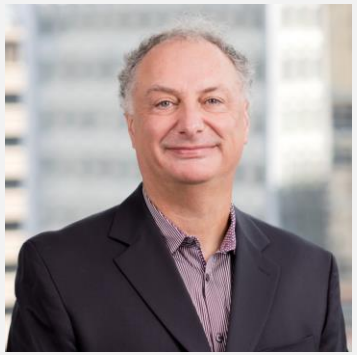
Speakers: Kirk J. Nahra, Arianna Evers, Shannon Togawa Mercer & Ali A. Jessani

Webinar Guidelines

- Participants are in listen-only mode
- Submit questions via the Q&A feature
- Questions will be answered as time permits
- Offering 1 CLE credit in California and New York*
- The webcast is being streamed through your computer, so there is no dial-in number. For the best quality, please make sure your volume is up and other applications are closed. If you experience a delay or get disconnected, press F5 to refresh your screen at any time
- For additional help with common technical issues, click on the question mark icon at the bottom of your screen

WilmerHale has been accredited by the New York State and California State Continuing Legal Education Boards as a provider of continuing legal education. This program is being planned with the intention to offer CLE credit in California and non-transitional credit in New York. This program, therefore, is being planned with the intention to offer CLE credit for experienced New York attorneys only. Attendees of this program may be able to claim England & Wales CPD for this program. WilmerHale has been approved as a Colorado Certified Provider, as recognized by the Colorado Supreme Court Continuing Legal and Judicial Education Committee. We will apply for Colorado CLE if requested. The type and amount of credit awarded will be determined solely by the Colorado Supreme Court. New Jersey grants reciprocal credit for programs that are approved in New York. We can also issue Connecticut credit for this program. All attendees, regardless of jurisdiction, will receive a uniform certificate of attendance that shows the states in which the program was approved. Attendees requesting CLE credit must attend the entire program. CLE credit is not available for on-demand webinar recordings.

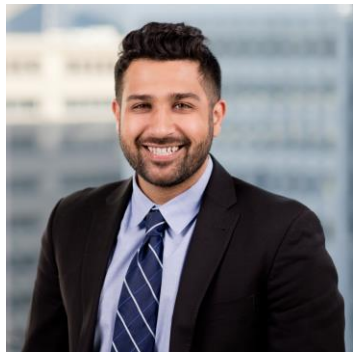
Speakers



Kirk J. Nahra
Partner
Co-Chair, Cybersecurity and Privacy Practice
WilmerHale

Arianna Evers
Counsel
WilmerHale

Shannon Togawa Mercer
Senior Associate
WilmerHale



Ali A. Jessani
Associate
WilmerHale

Overview

- **Prepare & Respond**
  - California's CCPA and CPRA, and other state law developments
  - FTC enforcement priorities and related issues
  - Privacy developments in the European Union
  - Health care and health information privacy developments
- **Anticipate**
  - Key expected developments in privacy in the above areas throughout the presentation, as well as prospects for federal privacy legislation

State Law Update

California Consumer Privacy Act (CCPA) Update

CCPA went into effect January 1, 2020; enforcement by the California AG began on July 1, 2020

- Final regulations were approved in August 2020
  - Additional modifications proposed in October 2020
- No announced enforcement decisions by the California AG's office, though some companies have received letters stating that they were non-compliant

CCPA Update

There have been a number of lawsuits brought under the CCPA's private right of action since January 1, 2020

Cases have been brought against companies for:

- Data breaches
- Failure to comply with the CCPA's privacy provisions
- California's unfair competition law

Introduction to the California Privacy Rights Act (CPRA)

CPRA voted into law on November 3, 2020

- Comprehensive privacy law that builds upon the CCPA and brings it somewhat more in line with the GDPR
- Proposed as a ballot initiative in 2019 by Alastair McTaggart (same person who initially proposed CCPA as a ballot initiative)
- Received over 55% of the vote
- The new requirements on businesses go into effect January 1, 2023, and apply to personal information businesses collect after January 1, 2022
- Enforcement begins July 1, 2023
- Regulations for the CPRA must be adopted by July 1, 2022

What is the CPRA?

Creates the **California Privacy Protection Agency (CPPA)** that is responsible for enforcing the CPRA

- Replaces the California AG for CCPA enforcement
- Responsible for rulemaking
- Funding and establishment of CPPA can begin as early as December 2020

Creates a new category of data called “sensitive personal information”

- SSN
- Financial information
- Precise geolocation information
- Biometrics
- Health information

Businesses must implement a “Limit the Use of My Sensitive Personal Information” link

What is the CPRA?

Expands on the individual rights created by the CCPA:

- Right to opt out of “sharing” (in addition to the right to opt out of sale)
- Right to correct
- Rights related to automated decision-making (similar to GDPR)
- Rights related to sensitive personal information
- Right to know expands beyond 12 months where not impossible or disproportionately burdensome

What is the CPRA?

- Creates a new "contractor" category and additional requirements for vendor contracts (for both contractors and service providers)
- Creates a "reasonable security" requirement for all personal information
- Implements data minimization and data retention requirements
- Triples fines for children's privacy violations
- Slightly expands private right of action to include "a consumer's email address along with a security question or password that would permit access to the consumer's account"
- "High risk" activities will require cybersecurity audits and privacy impact assessments

Other state law developments

- Number of privacy laws proposed in NY
- Washington Privacy Act of 2021 will be reintroduced
- We expect other states to also propose comprehensive privacy laws during the 2021 legislative session
- California has a unique history – unclear if other states will be able to pass comprehensive privacy legislation and little expectation that these laws will look like California

Bills to keep an eye out for in New York

It's Your Data Act

- Would create criminal penalties for certain data sharing activities

New York Privacy Rights Act

- Would create a fiduciary obligation for data controllers and private right of action

Privacy bill proposed by Governor Cuomo

- Will require businesses to only collect data for the purposes for which they need it

FTC Enforcement

FTC Enforcement Priorities – Biometrics

- ***Everalbum, Inc.***
  - Photo app that uses facial recognition technology to group users' photos by the faces of the people who appear in them and allows users to "tag" people by name
  - Facial recognition enabled by default; then different treatment for users depending on jurisdiction
  - Data sets used for development purposes
- Counts: misrepresentation about (1) users' ability to control the facial recognition feature, and (2) account deletion
- Settlement requires affirmative express consent and includes deletion requirements
- Other biometric developments
  - National Biometric Information Privacy Act
  - New York Biometric Privacy Act (Assembly Bill 27)
  - Municipal facial recognition bans

FTC Enforcement Priorities – Health Information

- ***Flo Health, Inc*.**
  - Period and fertility app used by 100 million customers
  - Disclosure to third-party marketing and analytics service providers
- Counts: misrepresentations about disclosures and limitations on third-party use, failure to adhere to Privacy Shield Framework Principles
- Settlement requires consumer notice and that Flo direct service providers to destroy users' health information
- Health Breach Notification Rule
- Software Development Kits ("SDKs")

FTC Enforcement Priorities – Gramm-Leach-Bliley

- ***Ascension Data & Analytics***
  - Analytics company that processed mortgage applications and associated documents with personal information of 60,593 consumers
  - Service provider misconfigured server and storage location leading to exposed records
- Violations of Gramm-Leach-Bliley ("GLB") Act's Safeguards Rule, which requires financial institutions to develop, implement, and maintain a comprehensive information security program
  - Failure to oversee service providers
  - Failure to conduct an adequate risk assessment
- Settlement requires implementation of comprehensive data security program, including annual third-party assessments
- FTC proposed amendments to GLB Safeguards Rule

FTC Enforcement Priorities – Data Security

- ***Zoom Video Communications, Inc.***
  - Misrepresentations regarding encryption
  - "ZoomOpener"
  - "Zoom-Bombing"
- Settlement requires implementation of specific security controls, oversight and reporting obligations, and prohibitions against privacy and security misrepresentations
- ***Skymed International, Inc.***
  - Unsecured cloud database containing person information for 130,000 records
  - Misleading notice to customers about the incident
  - "HIPAA Compliance" seal
- Settlement includes prohibitions on misrepresentations, consumer notice, and implementation of information security program

FTC Enforcement – Takeaways

- New commissioners and leadership
- More resources and attention from lawmakers
- Increased focus on using existing “tools” and litigating cases
- More specific requirements and more/longer oversight and reporting obligations
- Broader investigations
- Media and security researcher reports often spark investigations
- Actual or likely consumer harm
- Benchmarking
- Areas of interest: health information, children’s privacy, artificial intelligence, biometrics, IoT, service provider oversight


European Union

European Privacy Developments in 2020

- General Data Protection Regulation ("GDPR") Enforcement
- *Schrems II* and Privacy Shield Invalidation
- New European Commission Standard Contractual Clauses ("EC SCCs")
- "Brexit" and Data Flows

GDPR Enforcement

- European regulators imposed almost € 160 million in fines in 2020 (almost 40% of all GDPR fines imposed since May 25, 2018)
- Notable enforcement actions:
  - The U.K. Information Commissioner's Office ("ICO") levied fines of:
    - around £ 20 m (€ 22.2 m) for an airline "failing to protect the personal and financial details of more than 400,000" customers; and
    - around £ 18.4 m (€ 20.4 m) for a hotel group "failing to keep millions of customers' personal data secure" in the context of a security breach
  - First French *Commission nationale de l'informatique et des libertés* ("CNIL") fine reaching the enforcement stage of an investigation with the CNIL as Lead Supervisory Authority
  - Hamburg Commissioner for Data Protection fined a company nearly € 35.3 m for an internal breach

Schrems II and Privacy Shield Invalidation

- July 16, 2020, Court of Justice of the European Union issued its judgment in *Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems* (Case C-311/18) ("*Schrems II*")
  - Invalidated the EU-U.S. Privacy Shield Framework
  - Complicated validity of EC SCCs
  - Introduced significant uncertainty around international data transfers
- European Data Protection Board ("EDPB") issued Recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data
  - Accompanied by the European Essential Guarantees for surveillance measures
- What does this mean for companies in the U.S. importing EU data?

New EC Standard Contractual Clauses

- Draft new Standard Contractual Clauses were released on November 11, 2020
  - Provides for controller-to-controller; controller-to-processor; processor-to-processor; and processor-to-controller transfers
- EDPB and EDPS issued a joint opinion on new EC SCCs on January 15, 2021
  - Recommended redrafting to align with EDPB Recommendations on Supplementary Measures
- The European Commission will now have to make a final decision on the new SCCs
- Once they do, there is a one-year transition period for companies currently using the older versions of the SCCs

Brexit and Data Flows

- Why does Brexit create a problem for European data flows?
  - European Commission Adequacy Decisions under GDPR
  - As of January 1, 2021, the UK technically holds third-country status
- December 24, 2020: EU-UK Trade and Cooperation Agreement
  - Transition period of up to six-months (initial four months with a two-month extension)
- Beyond the transition period?
  - Divergence of UK GDPR, DPA 2018, and EU GDPR over time
  - Practical impact
- What should UK-based companies and organizations do now to prepare?
  - Adequate safeguards
  - Cross-border data transfer agreements

What to look out for in 2021

- Successor to EU-U.S. (and Swiss-U.S.) Privacy Shield Framework
- Enforcement of rules concerning international data transfers
  - Potential for increased data localization
- Increased scrutiny of surveillance measures in EU
- United Kingdom adequacy decision
- Other proposed acts and regulations related to the use of data:
  - ePrivacy Regulation
  - European Commission Strategy for Data and Regulation on European Data Governance
    - European Parliament Data Governance Act


Health Care Privacy

Evolution/Revolution for Health Care Privacy

- HIPAA Rules have set the benchmark for the health care industry for almost two decades — standard for the health care industry and consumers that has worked (mostly) well for both.
- Increasing challenges with the existing structure given a variety of changes in both the traditional health care industry and in the enormous concern with “unregulated” health data
- While HIPAA still works well where it applies (although this may be a controversial statement), there are increasing situations where it doesn’t fit
- And some situations — even in the core health care system — where it may not work well

Health Care Enforcement

- Health and Human Services Office of Civil Rights ("HHS OCR") — lots of activity, focus on patient access cases
- New potential disruption to HHS OCR enforcement approach from *M.D. Anderson Cancer Center* case
- States are watching— e.g., *Glow* case in California
- FTC is watching as well – e.g., *Flo* case
- Both regulated and "unregulated" health companies face meaningful enforcement risks (unregulated is a bit of a misnomer)

How is your health information protected in California?

1. HIPAA protected information (generally exempted from CCPA)
2. Confidentiality of Medical Information Act covered companies/information (generally exempted from CCPA)
3. Common Rule/Clinical research (generally exempted from CCPA)
4. CCPA — probably covers your health information if it isn't exempted
   - **BUT** CCPA doesn't cover non-profits
   - And CCPA doesn't generally cover employers and employee information
5. How can consumers, businesses and others deal with this?

Anticipated Privacy Developments – National Privacy Legislation

A different approach

- GDPR — Broad principles establishing data privacy and security law across the EU
- Protects all personal information in all settings
- Application to a wide range of US companies
- Health care industry simply part of the overall legislation
- Health care data considered sensitive information with certain special restrictions
- Not a recommendation but an alternative model

What is the Right Approach

- Should there be an “overall” approach to privacy, or something tailored to more specific situations?
- Compare CCPA approach (general, although with lots of exceptions) — to something like a facial recognition law
- HIPAA rules have careful nuance to make the health care system work well / same with GLB rules for financial services
- Our current laws deal with lots of different topics, activities, data categories and industries

Impact of COVID-19 – Some lessons

- Has highlighted the impact of employee privacy issues – where (in the US) there are few direct privacy laws (and the ADA is now something privacy lawyers and privacy officers need to know)
- Has highlighted a “weakness” in privacy law. Most privacy law addresses respective rights of data subjects and the entities they interact with (e.g., a bank and its consumers)
- COVID-19 has added the issue of impact of data sharing on third parties — others who might be impacted. Not really part of our privacy model
- In US, also has highlighted that there is essentially no law about the monitoring of “other” people — visitors, contractors, service providers, guests, customers

Key issues for legislative debate

- Preemption
- Private right of action
- Existing federal laws (and whether they will still apply)
- Scope of Individual Rights
- Permitted disclosures vs. areas where permission from consumers is needed
- Enforcement
- Coverage of employee data / “business to business” data

Key issues for legislative debate

- Dealing with innovation
- Broad scope of personal data
- Special protection for “sensitive” data (and how is that defined)
- Intention towards international principles
- Discrimination/Artificial Intelligence/Algorithms?
- Data security issues?
- Data Brokers?
- What other issues should be part of the debate?

Our prediction for federal privacy legislation

- Odds go up in 2021 — presumption is that a Biden Administration will be somewhat more interested in a privacy law but not a significant priority
- Some open issues because of Vice President Harris's role as California AG in the past
- Major driver will be the wild card of other states
- If 3-5 significant states pass "California-like" laws, then industry will need to support a federal law
- Our prediction — a meaningful chance (more than 50-50) of a national privacy law during this presidential term
- Enormous open questions of what this law would actually do and how it would interplay with other state and federal laws

Things to watch for

- If states start to move, will anything follow California?
- Will another state “model” emerge as the prototype?
- How broad will the discussions be on a federal law/How many topics will be included?
- What about discrimination/artificial intelligence/algorithm issues?
- How will existing federal laws be addressed? (exempted, supplemented, replaced)

Contact

Kirk J. Nahra
Partner; Co-Chair, Cybersecurity and Privacy Practice
WilmerHale
kirk.nahra@wilmerhale.com

Shannon Togawa Mercer
Senior Associate
WilmerHale
shannon.mercer@wilmerhale.com

Ali A. Jessani
Associate
WilmerHale
ali.jessani@wilmerhale.com

Arianna Evers
Counsel
WilmerHale
arianna.evers@wilmerhale.com

WilmerHale Privacy and Cybersecurity Law Blog

Twitter: @WHCyberPrivacy