What's Ahead in 2020 for Consumer Privacy?

January 15, 2020

Agenda

- **Welcome**
  - **Jennifer Covich Bordenick,** *CEO, eHealth Initiative*
- **Presentation:**
  - **Alice Leiter, JD,** *Vice President & Senior Counsel, eHealth Initiative*
  - **Alaap Shah, JD, MPH** *Member of the Firm, Epstein Becker and Green*
- **Q&A**
  - **Jennifer Covich Bordenick**, *CEO, eHealth Initiative*

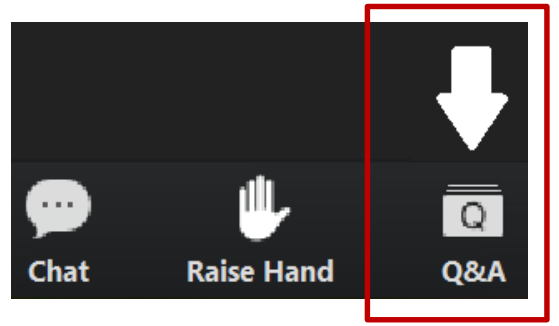
SPEAKERS

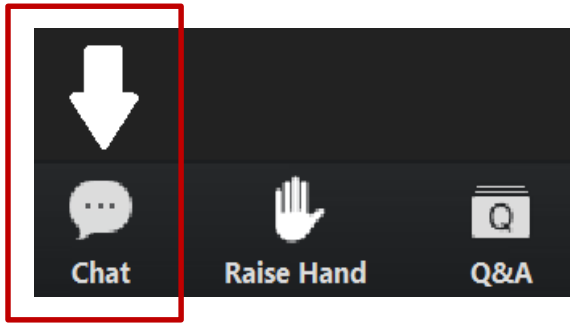
Alice Leiter, JD, Vice President & Senior Counsel, eHealth Initiative

Alaap Shah, JD, MPH
Member of the Firm
Epstein Becker and Green

Housekeeping

- **All participants are muted**
- **To ask a question to be answered by speakers:**
  - Use the “Q&A” box found on the bottom of your screen
  - We will address as many as possible after the presentations
- **For help with technical difficulties and non-speaker questions:**
  - Use the “chat” box and we will respond as soon as possible
- Slides and a recording of today’s presentation will be available for download on eHI’s Resource page: **www.ehidc.org/resources**





eHI's Mission

Convening executives from every stakeholder group in healthcare to discuss, identify and share best practices to transform the delivery of healthcare using technology and innovation.

Current Areas of Focus

Value-Based Care

- Cost Transparency
- Prior Authorization

Interoperability

- Understanding FHIR/ APIs/DaVinci
- Policy Issues/Burden, Workflow, Info Blocking

Privacy/Security

- Protection Vs. Access
- HIPAA Part 2
- Cybersecurity Med Devices

Analytics/SDOH

- Non-Traditional Sources of Data for Health (SDOH, PGHD)
- EHR Data for Clinical Trials (Doublejump)

eHealth Resource Center
www.ehidc.org/resources

- eHealth Resource Center available with best practices & findings identifying and disseminating best practices
- Online Resource Center: over 600 new pieces of content, 125 best practices added this year

Presented by

Alice Leiter, JD
Vice President & Senior Counsel eHealth Initiative & Foundation

Alice@ehidc.org

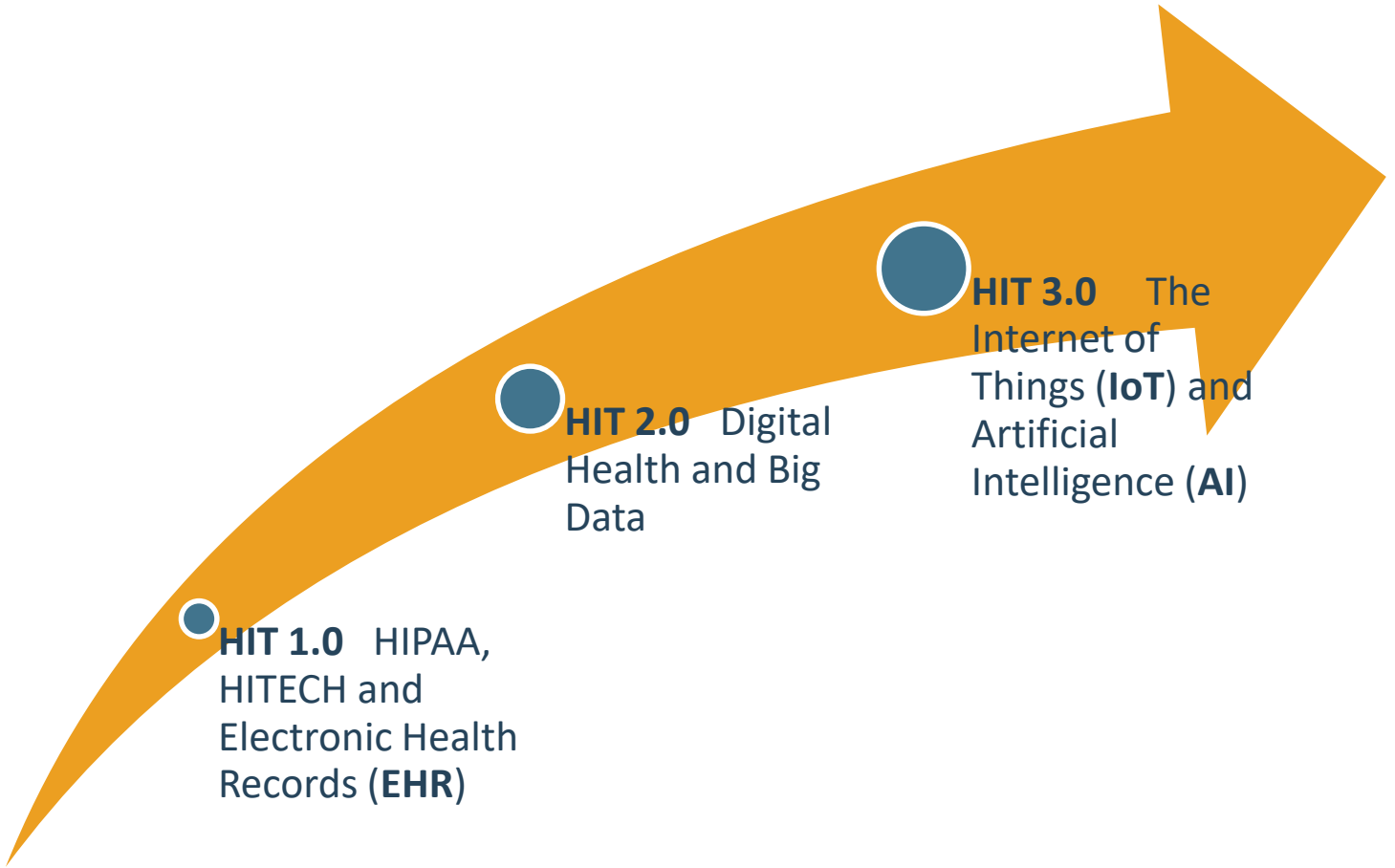
Presentation Agenda

- Consumerism in Healthcare
- HIPAA's Role in Consumer Directed Health
- ONC Proposed Rules on Interoperability
- Proposed Federal Privacy Legislation
- International Law
- State Law Developments

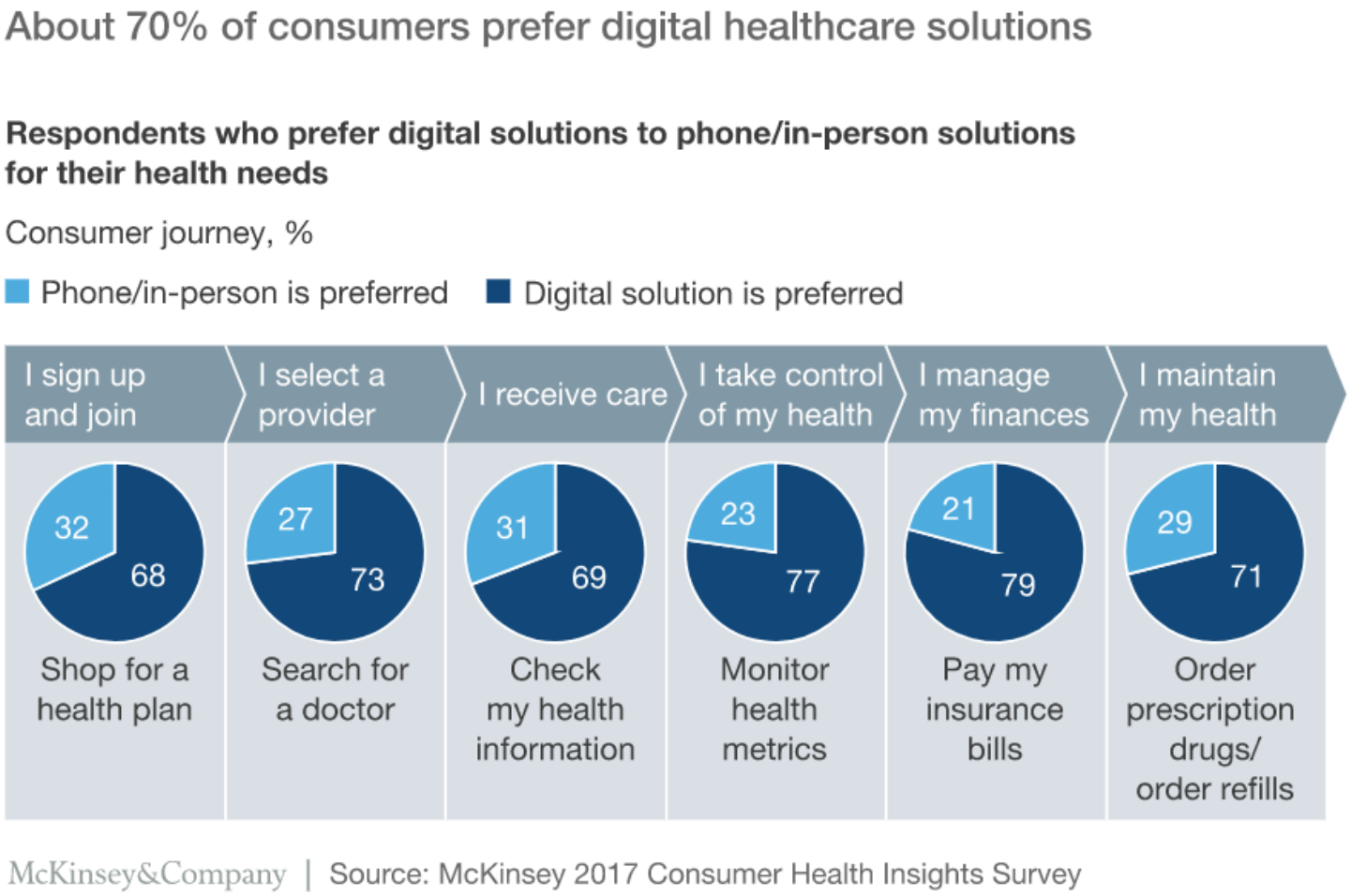
What's Driving the State of Consumer Health?

- Increasing consumer reliance on personal technology devices and platforms to manage individual health – most of which are NOT covered by HIPAA
- Rapid expansion of the volume of electronic health data
- Rapid expansion of the potential of digital medicine
- All are outpacing the ability of legislators and regulators to keep up; HIPAA is increasingly outdated, states are filling gaps
- Consumer enthusiasm *for* digital health is greater than consumer trust *in* digital health

Consumerism in Healthcare: Industry Evolution



Consumerism in Healthcare: Patient-Centric



What to Do About It?

- Close the gaps in HIPAA?
- Rely more on FTC enforcement?
- Or on state-level protections?
- Take cues from international law and pass comprehensive federal privacy legislation?
- Better consumer education/more transparency?
- Private-sector innovation or governance?

Presented by

Alaap B. Shah

Member of the Firm

Epstein Becker Green P.C.

ABShah@ebglaw.com

202.861.5320

My Background

- Member of the Firm, Epstein Becker & Green P.C.
  - Partner in Heath Care and Life Sciences Division
  - Co-Lead of Data Privacy, Cybersecurity and Data Asset Management Team
- American Society of Clinical Oncology/CancerLinQ
  - Senior Counsel, Chief Privacy and Security Officer
  - Helped launch CancerLinQ – Big Data in Oncology
  - Helped manage enterprise-wide risk associated with privacy and security
- Certified by IAPP as a Privacy Professional
- Certified by HIMSS as a Health Information Systems Professional
- Certified by HITRUST on the Common Security Framework

Consumerism in Healthcare: Data is King

The world's most valuable resource is no longer oil, but data.

- *"Alphabet, Amazon, Apple, Facebook and Microsoft . . . are the five most valuable listed firms in the world."*
- *"With data there are extra network effects. By collecting more data, a firm has more scope to improve its products, which attract more users, generating even more data, and so on."*
- *"They have a 'God's eye view' of activities in their own markets and beyond."*

The 'Data Economy' is at a fever pitch. Enormous value may be realized as long as data continues to flow and trust is maintained.

Credit: The Economist, May 6, 2017

Consumerism in Healthcare: Recent Headlines

Credit: Wall Street Journal – Jan. 11, 2020

At CES, Apple, Facebook and Amazon are preaching privacy. Don't believe the hype.

Privacy-washing is all the rage at tech's biggest event — and not what we need.

Credit: Washington Post – Jan. 8, 2020

Microsoft, Humana ink 7-year strategic partnership to leverage cloud, AI and voice technologies

by Heather Landi | Oct 21, 2019 10:05am

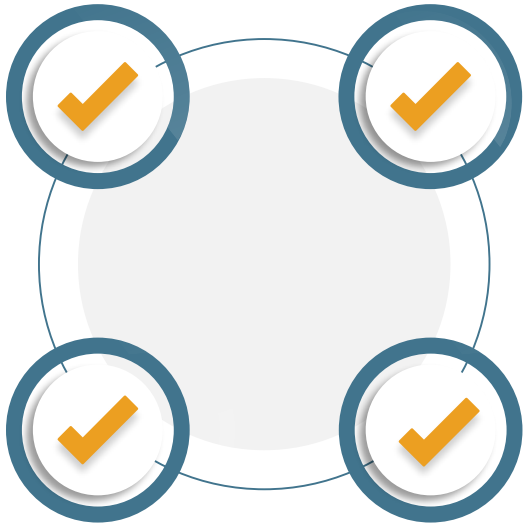
Humana wants to use cloud and artificial intelligence technologies to improve members' health outcomes and make their healthcare experiences simpler to navigate. (Microsoft)

Credit: FierceHealthcare – Oct. 21, 2019

HIPAA In a Nutshell . . .

The Privacy Rule regulates use or disclose of Protected Health Information ("PHI") and obligations to subjects of that information.

The Security Rule sets standards to protect the availability, integrity, and confidentiality of E-PHI



The Breach Notification Rule establishes obligations to report security incidents and breaches to various stakeholders

The Enforcement Rule establishes the penalty framework for HIPAA violations

Who is Subject to HIPAA?

Covered Entities	Business Associates

• **Health care providers:** providers of medical or health services who transmit health information in electronic form
 	
• **Health plans:**
  • Health insurers and HMOs
  • Insured and self-funded employee welfare benefit plans that have 50 or more participants or are administered by an entity other than the sponsor
 	
• **Health care clearinghouses:** billing services, re-pricing companies and others that engage in data translation
	• Performing functions or provides services involving PHI or maintains PHI on behalf of a Covered Entity
	
	• Broad scope of entities considered BAs
	
	• Examples:
	  • Cloud or software vendor who hosts software containing PHI
	  • Data analytics involving PHI
	  • Vendor support involving PHI
	  • Revenue cycle management
	  • Patient outreach activities
	  • Utilization review
	  • Quality Assurance
	  • Benefits management
	  • Legal/Accounting services

HIPAA's Role in Consumer Directed Health

- Individuals right to access PHI:
  - See recent HIPAA FAQ guidance
  - Including transmission to a 3rd party app
  - Cannot deny request based on privacy or security concerns of app
- Covered Entities that transmit PHI to a non-HIPAA covered apps will NOT be liable for subsequent unlawful uses or disclosure of that data
- Apps developed for or on behalf of a Covered Entity by a Business Associate will likely be covered by HIPAA
- OCR settles right of access cases
- Data sharing agreements with non-traditional entities (i.e. tech giants and 3rd party apps) will continue to garner attention

ONC Proposed Rules on Interoperability

- Proposed Rule issued on March 4, 2019 (pursuant to 21st Century Cures Act)
  - Prohibit Information Blocking with limited exceptions
- Geared toward promoting patient access and consumer-directed sharing of data to spur digital health innovation
- 4 sets of actors must comply with data blocking requirements
- New definition with widespread implications – "EHI" or electronic health information
- Big focus on APIs
- Final rule expected in Q1 or Q2 of 2020

Image Credit: Shutterstock

ONC Proposed Rules on Interoperability

- Improve certified EHRs including greater transparency around product capabilities and contracting (i.e. prohibitions on gag clauses, real world testing)
- To speed interoperability ONC is focusing on two use cases involving exporting "EHI." This would replace the CCDA data export certification criteria with a "standards agnostic" approach.
    1. **Patient access to data:** Enable the export of EHI for a single patient upon a valid request from that patient or a user on the patient's behalf.
    2. **Providers switching vendors:** When a healthcare provider chooses to transition or migrate information to another health IT system
- APIs
    - A key provision in the Cures Act calls for ensuring patients be able to access their information via APIs "without special effort."
    - Require EHRs to publish APIs and limit fees

FTC's Role in Consumer Directed Health

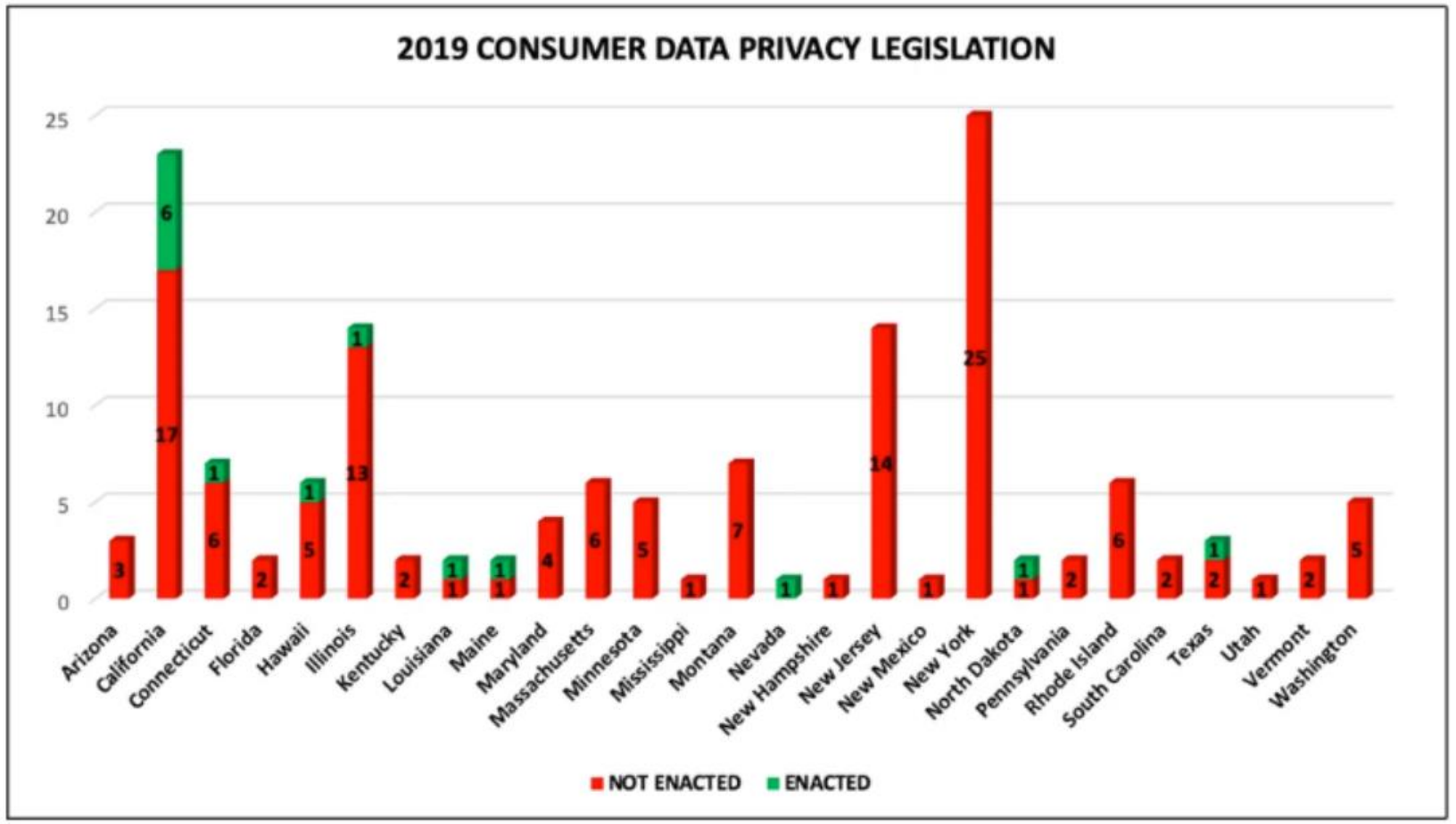
- Section 5 of the FTC Act
  - Prohibits unfair methods of competition and deceptive practices
  - FTC actions have been based on:
    - Failure to safeguard information;
    - Failure to adequately disclose to consumers how information will be used or disclosed;
    - Misrepresenting how information collected would be used
- FTC Privacy Expectations
  - Build privacy considerations in from the start
  - Be transparent about data practices
  - Offer choices that are easy to find and easy to use
  - Honor privacy promises
  - Collect sensitive information only with consent
  - Keep user data secure

International Law

General Data Protection Regulation

- Effective May 25, 2018
- Protects EU Resident Personal Data
  - Establishes transparency, notice and consent requirements
  - Right to Access
  - Right to Erasure
  - Establish data breach reporting requirements within 72 hours
- Extraterritorial Reach – applies to entities that control or process Personal Data even if such entities do not have a physical presence in the EU
- Stiff penalties – fines up to €20 million or 4% of global revenues

State Law Developments



Credit: MauriceWutscher: The 2019 Privacy Legislation Bomb Cyclone – Dec. 31, 2019

State Law Developments

- All 50 States (and the District of Columbia) have data breach notification and/or data security laws.
  - Variable definitions of Personal Information
  - Variable notification periods and triggers
- Trends in changes to breach notification and data security laws:
  - Expanding the universe of the type of data which must be protected and which triggers notification requirement to consumers in the event of breach
  - Imposing data security obligations
- Trends in State privacy laws:
  - California Consumer Privacy Act of 2018
  - Other states passing privacy legislation: IL (Biometric Information Privacy Act), NV (SB 220), NY (SHIELD Act), etc. . . .

State Law Developments

California Consumer Privacy Act (CCPA)

- Effective January 1, 2020 (but State AG signaled delayed enforcement
- Proposed Regulations issued but not yet final
- Requires a business that collects personal information from California consumers to disclose upon request:
  - Categories of personal information it collects;
  - The categories of sources from which it collects personal information;
  - The business or commercial purpose for collecting or selling personal information;
  - The categories of third parties with whom it shares personal information;
  - The specific personal information collected on the requesting consumer.
- Covered entities (under the HIPAA Privacy Rule) are exempted

Image Credit: Shutterstock

State Law Developments

California Consumer Privacy Act (CCPA)

- Consumer has a right to request deletion of any personal information with limited exceptions
- Consumer has right to direct business not to sell personal information ("opt out")
- Special protections for those under 16
- Several Amendments have passed in 2019 which modified the law
  - Employee data is currently not included in definition of personal information
  - Clarification that personal information does not include de-identified or aggregated data
  - Online-only businesses do not need to provide a toll-free number for consumer requests
  - Limits to private rights of action only if breach involved unredacted and non-encrypted data

Federal Privacy Legislation

116th Congress (2019-2020)

- Over 12 data and privacy related bills introduced in House and Senate
- As of Jan. 1, 2020 – all privacy bills remain under committee review
- Majority of the bills contain following elements:
  - Establish a private right of action
  - Create an independent data protection agency
  - Provide individuals right to access, control, and delete
  - Do not preempt stronger state laws
  - Require algorithm transparency (e.g AI, tracking and retargeting)
  - Adopt comprehensive definitions of personally identifiable information

Federal Privacy Legislation

116th Congress (2019-2020)

- **The Bill to Watch – Consumers Online Privacy Rights Act (COPRA)**
  - December 3, 2019 - Introduced on by Senator Maria Cantwell (D-WA)
    - Co-sponsors: Senators Schatz (D-HI), Klobuchar (D-MN), Markey (D-MA)
  - December 4, 2019 - Senate Committee on Commerce, Science, and Transportation, held hearing entitled, "Examining Legislative Proposals to Protect Consumer Data Privacy" to discuss proposed bills and specifically COPRA
- COPRA includes:
  - Explicit provision protecting state laws from preemption
  - Requires algorithmic decision-making impact assessments and prohibits bias and discrimination in advertising
  - Establishes a private right of action so individuals can enforce their rights, with damages for violations of act (no requirement to prove negligence or prove actual damage)
  - The Federal Trade Commission would enforce new privacy rules; allowed to fine companies for privacy violations

Federal Privacy Legislation

116th Congress (2019-2020)

Comparison of Privacy Bills based on Policy Provisions

Bill	Eshoo/ Lofgren	Cantwell	Wyden	Markey	Cortez-Masto	Rubio	Klobuchar -Kennedy	DelBene	Blackburn
Strong definition of personal data	✓	✓	✓	✓		✓		✓	✓
Establishes a Data Protection Agency	✓								
Individual rights (right to access, control, delete)	✓	✓	✓	✓	✓	✓			
Strong data controller obligations	✓	✓		✓	✓				
Algorithmic transparency requirements	✓	✓	✓						
Data minimization requirements	✓	✓		✓	✓				
Prohibits "take-it-or-leave-it" or "pay-for-privacy terms"		✓		✓	✓				✓
Private right of action for consumers	✓	✓	✓	✓					
Limits government access to personal data									
Does not preempt stronger state laws	✓	✓	✓	✓	✓		✓		

Credit: Grading on a Curve: Privacy Legislation in the 116th Congress (2019 -2020), Electronic Privacy Information Center (EPIC), Washington DC, available at https://www.epic.org/GradingOnACurve/EPIC-GradingOnACurve-Dec2019.pdf, (accessed Jan. 10, 2020).

Need for Regulatory Harmonization?

- HIPAA does not reach all actors . . .
- Movement of data from regulated to largely-unregulated actors . . .
- Lack of privacy and security regulation in third-party app space . . .
- Significant variability across privacy and security laws . . .
- Some states have begun to adopt more sweeping privacy legislation, but this will continue to foster a fragmented legal landscape . . .
- The Federal Government is considering overarching privacy legislation, but uncertain progress due to state of Congress and election year . . .

What does this mean for consumer privacy in 2020 . . . . ?

Credit: @carolinasquirrel on Etsy.com

Discussion Questions

- A recent survey, discussed at last week's CES tech summit, found that only about 38 percent of people believe proper safeguards are in place to protect their health data. Is federal legislation the best way to improve this statistic? (source: Digital Health Summit and Kantar, 2020)
- Given the overlaps in some of the privacy bills in the works, what are the most likely elements to make it to law?
- Short of successful federal legislation, what are things that individual stakeholders can do to shore up both consumer protections and increase public trust?


Bedankt
谢谢您
Thank you!
Grazie
Danke
Merci
謝謝您
Takk
Obrigado
Gracias

Q&A

Alice Leiter, JD, Vice President & Senior Counsel, eHealth Initiative

Alaap Shah, JD, Member of the Firm, Epstein Becker and Green