Contact Tracing Privacy Developments

Venable Privacy Law & Policy Webinar Series | July 23, 2020

Kelly DeMarchis Bastide
Partner
+1 202.344.4722
kabastide@Venable.com

Tara Sugiyama Potashnik
Partner
+1 202.344.4363
tspotashnik@Venable.com

Adriana Beach
Associate
+1 415.343.4501
aabeach@Venable.com

VENABLE LLP

Speakers

Kelly DeMarchis Bastide
Partner
+1 202.344.4722
kabastide@Venable.com

Tara Sugiyama Potashnik
Partner
+1 202.344.4363
tspotashnik@Venable.com

Adriana Beach
Associate
+1 415.343.4501
aabeach@Venable.com

VENABLE LLP

Agenda

1. What is contact tracing?
2. What privacy considerations does contact tracing raise?
3. Patchwork of regulations
    - Federal regulations
    - State regulations
    - Influential industry standards
4. How is federal legislation responding?
5. Takeaways
6. Questions

VENABLE LLP

What Is Contact Tracing?

VENABLE LLP

Contact Tracing Answers “Who?” and “How?”

- Who?
  - Who has contracted COVID-19 and who has interacted with them
- How?
  - How COVID-19 has spread and is spreading
- Contact tracing occurs both manually and automatically
  - We are focusing on automated methods

VENABLE LLP

Contact Tracing Raises Privacy Considerations

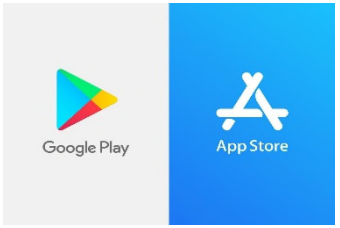
- Health information
- Location data
- Social network data
  - Paints an intimate picture of an individual's social circles
- Discriminatory tracking based on race
- Balancing anonymity and public safety
- Data storage – Centralized or Decentralized?
- Technical questions of operationalizing privacy for example:
  - Tracking location via GPS versus tracking proximity via Bluetooth
  - Tracking location and health-related data via Wearables
- Existing industry standards for contact tracing

VENABLE LLP

A Patchwork of Laws and Regulations

VENABLE LLP

Sources of Laws and Regulations



Federal and state laws and regulations, as well as industry standards, will govern the use of contact tracing apps

- Federal Trade Commission (FTC)
- States
- Industry Standards

VENABLE LLP

Federal Laws and Regulations

- The FTC regulates privacy under its consumer protection authority to protect against unfair and deceptive acts or practices in Section 5 of the FTC Act
- FTC on collection, data minimization, and notice:
  - Apps' privacy polices are notice and must accurately describe collection practices
  - Acting beyond policy terms may trigger an enforcement action
  - FTC on consent:
- Apps should obtain consumers' consent for material updates to privacy policies, prior to collection and use of data of consumers
- FTC on data security:
  - Inadequate security practices may trigger enforcement actions
- The FTC also offers guidance on
  - What constitutes deidentification
  - Avoiding use of personal information when not necessary
  - Precise location data as sensitive information requiring consent to collect

VENABLE LLP

Federal Laws and Regulations

- HIPAA applies to covered entities, including health care providers, health plans, and health care clearinghouses
  - Covered entities must consider their use and disclosure of protected health information
  - State rules may reference HIPAA
- Other sectoral laws may apply in certain circumstances, for example:
  - The Gramm-Leach-Bliley Act (GLBA) may affect financial institutions involved in contact tracing
  - The Children's Online Privacy Protection Act (COPPA) may affect apps collecting and using data collected from children online
- Federal communications privacy and wiretap laws such as the Stored Communications Act and Wiretap Act restrict access to stored and transmitted communications
  - There are state analogs to these laws

VENABLE LLP

State Laws and Regulations

- Commercial privacy policy laws in California, Delaware, and Nevada
  - Require an online privacy policy specifically covering data collection and use
- California Consumer Privacy Act (CCPA) notice obligations:
  - Require disclosing types of personal information collected and purposes for use
  - Require notice before using collected information for additional purposes
  - Say that a link to the notice may appear on the download page and in the app
  - Require just-in-time notices for collection of personal information for a purpose the consumer would not reasonably expect

VENABLE LLP

State Laws and Regulations

- Certain state laws create individual rights with respect to data
  - CCPA: rights to access, to delete, and to opt out of the sale of personal information
  - Maine: a customer must give express, affirmative consent to internet service providers before they use, disclose, sell, or permit access to the customer's personal information
  - Nevada: right to opt out of the sale of personal information
- Data security laws exist in at least 25 states
  - Affect state agencies and commercial entities

VENABLE LLP

Influential Industry Standards

- The Apple and Google Exposure Notification System (AGENS) will be the basis for multiple apps developed by health care authorities (Clover)
  - AGENS uses Bluetooth to track proximity rather than GPS to track locations
  - It tests “matches” on-device, notifying without revealing personal information
- Apple and Google also have influence via their app stores, requiring:
  - Notice and consent for data collection and sharing
  - Restrictions on secondary uses of data
  - Ability to restrict access to location, contacts, camera, microphone, and device storage
  - Data security
- Apple specifically requires the ability to revoke consent to collection, use, or disclosure of data

VENABLE LLP

Influential Industry Standards

Digital Advertising Alliance Principles

- Require consent for collection, use, and transfer of precise location data for certain purposes
- Also define principles for
  - Multi-site data
  - Cross-app data
  - Personal directory data
  - Purpose limitations
  - Restrictions on uses for eligibility purposes
  - Sensitive data
  - Security
  - Accountability

VENABLE LLP

Takeaways

- Unfair or deceptive acts and sectoral requirements implicate federal regulations
  - Data collection, notice, consent, and data security missteps may bring about FTC enforcement
  - Operating in certain industries or while interacting with a certain group's data may trigger sectoral privacy mandates
- Some states grant individual rights that expand on state protections related to collection, notice, consent, and security
- Industry standards from Apple, Google, and others influence marketplace practices
- This patchwork of laws does not create a unifying standard

VENABLE LLP

How is Federal Legislation Responding?

VENABLE LLP

Tracking Federal Legislation: A Sampling

Bill No. /Sponsor	Bill Title	Purpose of Bill	Latest Action
S. 3861 Cantwell (D-WA)	Exposure Notification Privacy Act	A bill to establish privacy requirements for operations of infectious disease exposure notification services.	6/1/20 – Introduced and referred to Senate Commerce
S. 3749 Blumenthal (D-CT)	Public Health Emergency Privacy Act *Companion measure H.R. 6866	A bill to protect the privacy of health information during a national health emergency.	5/14/20 – Introduced and referred to Senate Health, Education, Labor, and Pensions
H.R. 6866 Eshoo (D-CA)	Public Health Emergency Privacy Act *Companion measure S. 3749	A bill to protect the privacy of health information during a national health emergency.	5/14/20 – Introduced and referred to House Energy and Commerce
S. 3663 Wicker (R-MS)	COVID-19 Consumer Data Protection Act of 2020	A bill to protect the privacy of consumers' personal health information, proximity data, device data, and geolocation data during the coronavirus public health crisis.	5/7/20 – Introduced and referred to Senate Commerce

VENABLE LLP

Proposed Legislation

Bill No. /Sponsor	Deidentification	Deletion	Compliance with Legal Obligations	Breach Notification
S. 3861 Cantwell	Implies but does not define deidentification. Defines aggregate data	Does not address aggregation or deidentification as sufficient	Allows data transfer to satisfy legal duties. Silent on retention for legal duties and exempting legal duties from deletion requirement	Requires breach notification for covered data, not preempting existing law
S. 3749 Blumenthal / H.R. 6866 Eshoo	Defines neither deidentified nor aggregate data	Counts data not linkable to an individual as deletion	Creates carveouts for legal duties	No
S. 3663 Wicker	Defines both deidentified and aggregate data	Counts deidentification as deletion	Creates carveouts for legal duties	No

VENABLE LLP

Proposed Legislation

Bill No. / Sponsor	Scope of Automated Exposure Notification Service and Service Provider requirements	Non-discrimination	Preemption
S. 3861 Cantwell	Unclear on (1) dual purpose data and (2) use of data collected for another purpose in these systems	Prohibits mandatory denial of entry to a public accommodation for failure to participate	No
S. 3749 Blumenthal / H.R. 6866 Eshoo	Does not contain similar reporting requirement for service providers	Contains the same prohibition as Cantwell	No
S. 3663 Wicker	Does not contain similar reporting requirement for service providers	Contains the same prohibition as Cantwell but has exception for employees	Yes

VENABLE LLP

Takeaways

VENABLE LLP

Final Takeaways

- Contact tracing apps are a powerful evolution in public health to tackle the coronavirus pandemic
- Privacy and public health considerations contribute to usage and quality of contact tracing
- The current patchwork of laws means providers must consider each level of regulation in designing and operating apps
- Industry standards play a powerful role in the evolving marketplace
- Federal legislation proposals could grow and borrow from each other to better help the marketplace meet the privacy and public health challenges of contact tracing

VENABLE LLP

Thank You! Questions?

VENABLE LLP

VENABLE LLP