

Digital Content Next

Legal and Legislative Committee
February 12, 2019

Review of DCN Framework for Consumer Privacy Legislation

DCN Privacy Framework

Preemption

Transparency

Choice

Platforms

Data Security

Preemption

- Federal law should preempt state laws

Transparency

- Companies should state in plain terms what consumer data they collect, how they use the data and what choices they offer consumers

Consumers enjoy fundamental choice about whether to visit a website and app

- 1st party data collection/use meets with consumer expectations

Consumers should have control over data collection outside of their expectations

- Data collection by 3rd parties should be subject to choice mechanism
- Exceptions for fraud/security, billing, audience measurement, contextual advertising
- 3rd parties should be held liable for compliance and data security requirements

Companies must gain affirmative consent from consumer before selling consumer data

- “sale” defined narrowly

Intermediaries (platform companies that can see all or substantially all of a consumer's behavior)

- Must gain affirmative consent for any secondary use of data
- Cannot require consent for use of service
- Must not use market power to compel companies to agree to unfair terms or gain consent on their behalf

Companies should ensure consumer data is properly secured.

- The level of security should be proportionate to the sensitivity or breadth of the data held
- Safe harbor protection for complying with a standard
- Obligations and liability fall to the company that collects the data
- Browsers/Devices should be required to provide strong security
- 3rd parties should inform 1st parties when and why they are collecting data

Other Issues?
