manatt

A National Privacy and Data Security Game Changer

California Consumer Privacy Act

Thomas R. McMorrow, Brandon P. Reilly and John V. Trevino, Jr.

October 17, 2018

Introduction

Thomas R. McMorrow

Partner
tmcmorrow@manatt.com

Tom chairs the firm's California Policy and Regulatory Practice Group. He is generally retained to resolve intractable issues without the need for litigation or a political fight. Tom was one of the four private sector lawyers who successfully negotiated the terms of California's original Financial Services Privacy Act on behalf of financial services companies. He has also been active in negotiating elements of the state's many subsequent privacy protection laws.

Brandon P. Reilly

Associate
breilly@manatt.com

Brandon is a civil litigator and privacy and data security attorney counseling businesses and organizations on a wide range of issues in the privacy, data security and consumer financial services spaces. He advises clients on security incident investigation, containment and mitigation; managing data breach responses; and he assists impacted entities before and during litigation, regulatory inquiry and government enforcement.

John V. Trevino, Jr.

Counsel
jtrevino@manatt.com

John's practice focuses on commercial litigation, privacy and data protection, and other cybersecurity issues. John has worked as an in-house privacy and compliance attorney in corporate legal departments of major telecommunications, travel and technology companies and as a data privacy officer, where he designed and implemented data governance strategies and identified privacy-related enterprise risks.

Agenda

Introduction

Political Backdrop

State and Federal Landscape

Key Provisions

Changes from the Clean Up Legislation

Consequences of Noncompliance

How Does It Compare to GDPR?

Open Questions

Expected Future Legislation

Q&A

Political Backdrop

- Alastair Mactaggart forms Californians for Consumer Privacy (CCP)
- Late 2017, the "California Consumer Personal Information Disclosure and Sale Initiative" receives official title and summary
- May 2018, the CCP submits more than double the signatures required to qualify the Initiative for the November 2018 ballot
  - Business interests immediately mobilize to prevent the Initiative from becoming law
  - California State Senator Robert Hertzberg proposes an alternative to Mactaggart
  - In late June, Mactaggart finally agrees to a legislative alternative if enacted by June 28
- On June 25, the CCPA is first circulated publicly
- On June 27, the California Senate and Assembly unanimously approve the CCPA
- On June 28, Gov. Brown signs the CCPA into law
- On Sept. 23, Gov. Brown signs SB 1121 into law to "clean up" ambiguities in the CCPA

Agenda

Introduction

Political Backdrop

State and Federal Landscape

Key Provisions

Changes from the Clean Up Legislation

Consequences of Noncompliance

How Does It Compare to GDPR?

Open Questions

Expected Future Legislation

Q&A

- California
  - Data Breach Notification Law (2002, 2007, 2011, 2013–17)
  - Online Privacy Protection Act / “CalOPPA” (2003, 2013)
  - Financial Information Privacy Act (2003)
  - “Shine the Light” Law (2003)
  - Security Procedures and Practices (2004, 2014–15)
- Federal
  - Health Information Portability and Accountability Act / “HIPAA” (1996)
  - Children’s Online Privacy Protection Act / “COPPA” (1998)
  - Financial Services Mondernization Act / “GLBA” (1999)
  - CAN-SPAM (2003)
  - FTC and FTCA

Agenda

Introduction

Political Backdrop

State and Federal Landscape

Key Provisions

Changes from the Clean Up Legislation

Consequences of Noncompliance

How Does It Compare to GDPR?

Open Questions

Expected Future Legislation

Q&A

Key Provisions

- Applicability
  - Must be for-profit business
  - Must process data of California residents, and
  - One of the following must be true:
    - Annual revenues > $25 million;
    - Obtains PI of 50,000 or more CA residents annually; or
    - Derives 50%+ annual revenue from selling CA residents' PI
- Exceptions
  - Legal compliance
  - Commercial conduct "wholly outside" CA
  - HIPAA
  - GLBA
  - Credit reporting

Key Provisions

- Personal information
  - "[I]nformation that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."
  - Non-exhaustive list:

Name	Mail address	Phone number	Email address	IP address	Account info
SSN	Driver's license	Passport number or other ID	Biometrics	Geolocation	Protected classifications
Financial information	Medical information	Health insurance information	Commercial information	Education	Employment
Internet activity, browsing, search	Physical characteristics	Visual	Audio	Thermal	Olfactory

  - Catch-all: "Inferences drawn from any [of the above] to create a profile about the consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes."

- *Excludes*: De-identified or aggregated information; public information*

Key Provisions

- Right to access
  - Collected data: Categories and specific pieces of information; sources; purpose(s)
  - Shared data: Same, plus information disclosed and third parties receiving
  - Exception: One-time transactions
- Right to opt-out of sales
  - “Do Not Sell My Personal Information” button
  - Up to age 16: Must opt-in
  - Must expressly reauthorize after opting out
  - May not request reauthorization within 12 months of opt-out
- Right to deletion
  - Carve-outs: Complete transaction; breach/fraud protection; research; speech; internal analytics; legal compliance

Key Provisions

- Right to portability
  - Disclosures in “readily usable format”
- Nondiscrimination
  - May offer tiers of services/products for more data
- Privacy notices
  - Description of all rights
  - Clear and conspicuous opt-out link
  - Two-plus methods for requests; at minimum, a toll-free phone number and website address
- Verifiable requests
  - Requests must be reasonably verifiable
  - Respond within 45 days of receipt
- Separate homepages allowed

Agenda

Introduction

Political Backdrop

State and Federal Landscape

Key Provisions

Changes from the Clean Up Legislation

Consequences of Noncompliance

How Does It Compare to GDPR?

Open Questions

Expected Future Legislation

Q&A

Changes from the Clean Up Legislation

- Potential bifurcated implementation for certain provisions:
  - Potentially delays enforcement of the consumer information and use provision by the Attorney General until it adopts implementing regulations, but in any case no later than July 1, 2020.
  - The private right of action for data breach remains effective January 1, 2020
- Clarifies private right of action:
  - Only applies to data breach provisions
  - No requirement to notify the Attorney General before filing suit
- Exempts PI collected pursuant to Gramm-Leach-Bliley Act and the California Financial Information Privacy Act
- Addresses several prior ambiguities and inconsistencies:
  - Attorney General's available civil penalties
  - Clarifies exemption for data collected pursuant to HIPAA, CMIA and clinical trials
  - Remaining ambiguity on health provider liability – exemption only applies to the extent provider or covered entity "maintains patient information in the same manner" as required by HIPAA and the Health Information Technology for Economic and Clinical Health Act

Agenda

Introduction

Political Backdrop

State and Federal Landscape

Key Provisions

Changes from the Clean Up Legislation

Consequences of Noncompliance

How Does It Compare to GDPR?

Open Questions

Expected Future Legislation

Q&A

Consequences for Noncompliance

- Consumer Information and Use
  - Enforceable by California Attorney General
  - Not subject to private right of action
  - 30-day right to cure
  - Up to $2,500 per violation (via Unfair Competition Law)
  - Up to $7,500 per intentional violation (via CCPA)
- Data Breaches
  - Enforceable by California Attorney General and by private right of action
  - 30-day right to cure
  - $100–$750 in statutory damages per incident, per consumer ***or*** actual damages if greater
- Secondary Litigation Risks
  - Plaintiffs' counsel are expected to test for additional means of liability
  - One path will likely be complaints brought under California's Unfair Competition Law

Agenda

Introduction

Political Backdrop

State and Federal Landscape

Key Provisions

Changes from the Clean Up Legislation

Consequences of Noncompliance

How Does It Compare to GDPR?

Open Questions

Expected Future Legislation

Q&A

How Does It Compare to GDPR?

	GDPR	CCPA
Extraterritorial reach	(1) Establishment; (2) Offer goods/services; or (3) Monitor individuals	(1) Business in CA; and (2) Processes data of CA residents
Role differentiation	Controllers Processors	Businesses Service Providers Third Parties
Data	"…relating to an identified or identifiable natural person" Special categories	"…that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." No special categories

How Does It Compare to GDPR?

	GDPR	CCPA
Processing requirements	Prescriptive	Proscriptive
Right to access/know	Data processing practices	Re: collected data Re: shared data
Right to erasure	Broad	More limited
Right to correction	Right to rectify Right to object	None
Right to data portability	Broad	More limited
Right to opt out	Right to restrict processing	Right to opt out of data sales *Minors

How Does It Compare To GDPR?

	GDPR	CCPA
Anti-discrimination	Cannot discriminate based on exercise of rights	Same; *but* allows "financial incentives"
Enforcement	Member state DPAs Up to €20 million or 4% total worldwide annual turnover	California AG Up to $7,500 per violation
Private right of action	Yes, for damages	Breaches only, $100–$750 statutory damages or actual damages
Exemptions	Personal activity Government activity	Compliance with law De-identified/aggregated data HIPAA PHI GLBA NPI Credit reports

Agenda

Introduction

Political Backdrop

State and Federal Landscape

Key Provisions

Changes from the Clean Up Legislation

Consequences of Noncompliance

How Does It Compare to GDPR?

Open Questions

Expected Future Legislation

Q&A

Open Questions

- Philosophical flaws
  - Impact on low-cost and cost-free web services
  - Disproportionate burden on midsize and smaller businesses
- Nondiscrimination vs. financial incentives
- Data from past year – start complying 1/1/19?
- Definition of “sale”
  - “Other valuable consideration”

Open Questions

- Definition of data breach
  - Both broader and narrower than existing breach notification law

Breach notification law	CCPA breach action
Any CA resident "whose unencrypted personal information was, or is reasonably believed to have been, ***acquired by an unauthorized person***."	"Any consumer whose nonencrypted or nonredacted personal information…is subject to an unauthorized access and exfiltration, theft, ***or disclosure*** as a result of the business' violation of ***the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information***…"

  - Apparent reference to California Records Act
  - *LabMD v. FTC* (June 2018)

- What is a “cure”?
  - 30 days to “actually cure”
  - Express written statement of no further violations

Agenda

Introduction

Political Backdrop

State and Federal Landscape

Key Provisions

Changes from the Clean Up Legislation

Consequences of Noncompliance

How Does It Compare to GDPR?

Open Questions

Expected Future Legislation

Q&A

Expected Future Legislation

- Anticipate further attempts to modify the CCPA when California's legislature returns for its 2018–2020 session
- Attorney General is concerned on multiple fronts and may seek fixes
  - AG has noted "serious operational challenges" to its enforcement capacity
  - AG requested an expanded private right of action that was not adopted
  - AG not convinced implementing regulations can be in place by July 2020
- Commercial interests and consumer advocates also concerned
  - Business interests see the law as incompatible with existing state and federal law
  - Consumer advocates want to expand the rights of consumers under the CCPA
- Further changes are inevitable but unpredictable given evolving concepts of privacy across generations and nationally
- Federal preemption?

Agenda

Introduction

Political Backdrop

State and Federal Landscape

Key Provisions

Changes from the Clean Up Legislation

Consequences of Noncompliance

How Does It Compare to GDPR?

Open Questions

Expected Future Legislation

Q&A

Thank you!

Thomas R. McMorrow

Partner

tmcmorrow@manatt.com

Tom chairs the firm's California Policy and Regulatory Practice Group. He is generally retained to resolve intractable issues without the need for litigation or a political fight. Tom was one of the four private sector lawyers who successfully negotiated the terms of California's original Financial Services Privacy Act on behalf of financial services companies. He has also been active in negotiating elements of the state's many subsequent privacy protection laws.

Brandon P. Reilly

Associate

breilly@manatt.com

Brandon is a civil litigator and privacy and data security attorney counseling businesses and organizations on a wide range of issues in the privacy, data security and consumer financial services spaces. He advises clients on security incident investigation, containment and mitigation; managing data breach responses; and he assists impacted entities before and during litigation, regulatory inquiry and government enforcement.

John V. Trevino, Jr.

Counsel

jtrevino@manatt.com

John's practice focuses on commercial litigation, privacy and data protection, and other cybersecurity issues. John has worked as an in-house privacy and compliance attorney in corporate legal departments of major telecommunications, travel and technology companies and as a data privacy officer, where he designed and implemented data governance strategies and identified privacy-related enterprise risks.