womblebonddickinson.com

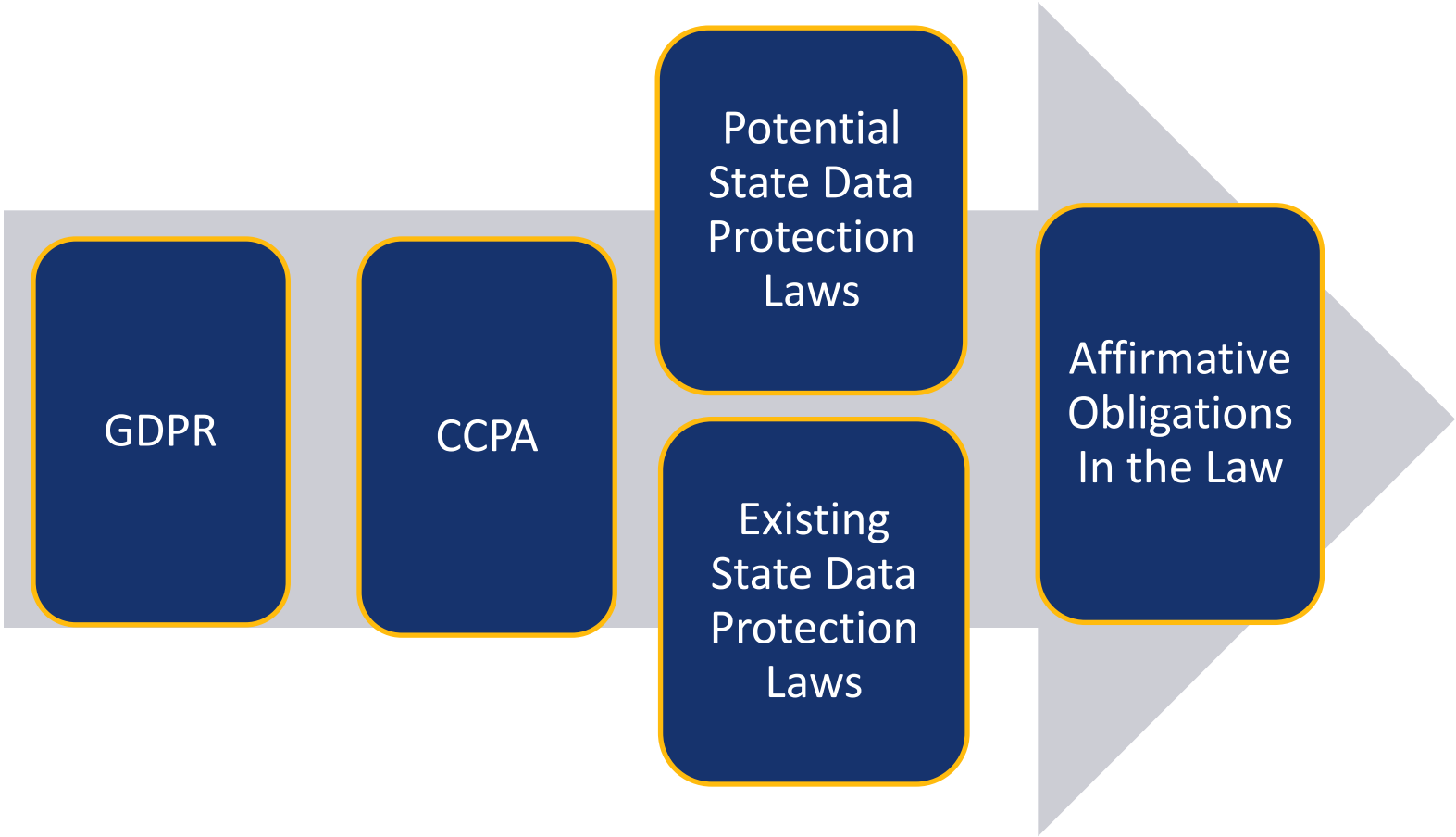
WOMBLE BOND DICKINSON

Beyond Breaches: Affirmative State Law Duties to Protect Data

Philip Gura
Dominic Panakal

May 14, 2019

Agenda


GDPR
CCPA
Potential State Data Protection Laws
Existing State Data Protection Laws
Affirmative Obligations In the Law

Changes in Attitudes: Crying Over Spilled Milk Vs. Locking the Barn Door

- GDPR, CCPA signal new *prospective* focus on privacy rights
- State laws until now mostly dealt with data breach response
- At least 10 states have considered or are considering omnibus privacy regulation
- Some states have current affirmative data duties
  - Information Security
  - Record Destruction
  - Restrictions on SSN

GDPR – General Data Protection Regulation

- Went into effect May 25, 2018
- Most comprehensive privacy law in the world
- Privacy by design
- Fundamental privacy rights
- Fines: €20 million or 4% of annual global revenue

Principles and Rights Under the GDPR

- **Notice**—data subjects should be given notice when their data is being collected;
- **Purpose**—data should only be used for the purpose stated and not for any other purposes;
- **Consent**—data should not be disclosed without the data subject's consent;
- **Accountability**—data subjects should have a method available to them to hold data collectors accountable for not following the above principles
- **Security**—collected data should be kept secure from any potential abuses;
- **Disclosure**—data subjects should be informed as to who is collecting their data;
- **Access**—data subjects should be allowed to access their data and make corrections to any inaccurate data;
- **Forgotten**—data subject right to be forgotten
- **Rights Exercised Free of Charge**

CCPA – California Consumer Privacy Act

- Most comprehensive privacy law in the U.S.
- Signed on June 28, 2018
- Revised September 23, 2018
- Goes into effect **January 1, 2020**

CCPA – Applicability & Key Components

1. A for-profit entity that;
2. Doing business in California; or
3. That collects personal information of California residents; and
4. Meets revenue thresholds *or* possesses PI of 50,000 California residents

1. Right to know
2. Right to access
3. Right to deletion
4. Right to opt-out
5. Right to equal service

CCPA Basics

- Applies to businesses *without* offices or employees in California
- Reaches activities conducted *outside* of California
- $2,500 per violation; $7,500 per intentional violation
- Limited private right of action
  - 30 days to cure
  - Up to $750 per consumer per incident or actual damages, whichever is greater
  - Note: Awaiting enforcement guidance from CA AG

CCPA – Recent Noteworthy Updates

- CA Attorney General held public hearings & took comments; regulations to follow
- SB 561: Another amendment introduced
  - Removes pre-enforcement 30 day right to cure
  - Adds a **private right of action** to *any* consumer whose rights are violated
  - An area that is constantly developing

CCPA and GDPR Are Influencing Other States

- At least 10 states are considering omnibus privacy legislation
- These state proposals include some of the following data rights:
  - Access to Collected Information
  - Access to Shared Information
  - Deletion
  - Portability
  - Opt-out
  - Age-Based Opt-in
  - Notice Requirement
  - Against Discrimination

CCPA and GDPR Are Influencing Other States

- Data Rights Common in Omnibus Proposals (Hawaii, Rhode Island, and Washington):
  - Access to Collected/Shared Information

    - Consumer has rights to request information about the processing, disclosure and/or sale of their personal information, and being notified of these rights in a public-facing privacy notice

  - Deletion

    - Grants consumers the right to request deletion of their personal information. Entities must disclose this right to consumers.

CCPA and GDPR Are Influencing Other States

- Data Rights Common in Omnibus Data Proposals (Hawaii, Rhode Island, and Washington)
  - Portability

    - Requires businesses list the categories of personal information that it sells/discloses to each category of third party to which the consumer's personal information is sold/disclosed.

  - Opt-out

    - Gives consumers the ability to direct a business not to sell their personal information to a third party. This section does not stop a business from distributing the data within the organization that collected it

  - Age-Based Opt-in

    - A business can only sell the personal information of a child between the ages of 13 and 16 with the child's consent and can only sell the personal information of a child under 13 with the consent of the child's parent or guardian.

  - Against Discrimination

    - Prohibits discrimination against consumers for exercising rights under the CCPA

One Big Issue: Two Approaches to Data Obligations

California embraced the GDPR style of data regulation

- Large Scale
- Comprehensive

North Carolina and other states are taking a different approach

- Smaller Scale
- Subject To Oversight
- Less California, More Alabama

We'll Know It When We See It – North Carolina

North Carolina - HB 904 would require that businesses "[i]mplement and maintain reasonable security procedures and practices, appropriate to the nature of the personal information and the size, complexity, and capabilities of the business, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

Despite not being omnibus, this creates a series of compliance hurdles

Existing Data Obligations – Information Security

- Many states require companies to take reasonable measures to implement and maintain security measures (i.e. Utah and Arkansas)
  - Not omnibus or comprehensive like California
  - Creates an affirmative information security obligation
  - Look to both Alabama and Ohio laws to understand industry standards and expectations

Information Security – Ex: Alabama

- Take reasonable measures to implement and maintain security measures, including consideration of the following:
  - (i) designation of an employee to coordinate the entity's security measures,
  - (ii) identification of risks for security breaches,
  - (iii) adoption of appropriate safeguards to address the identified risks and assess their effectiveness,
  - (iv) contractual retention of service providers to provide appropriate safeguards for personally identifiable information,
  - (v) adjustment of security measures for personally identifiable information to account for changes of circumstance, and
  - (vi) keeping the entities management informed of the security measures

  AL S.B. 318

Ohio's Affirmative Defense: How High Is High?

- Ohio's safe harbor applies to businesses that access, maintain, communicate or process personal or restricted information. Aimed at combatting the uptick in costly data breaches, cybersecurity measures must be designed to (i) protect the security and confidentiality of personal information; (ii) protect against any anticipated threats or hazards to the security or integrity of personal information; and (iii) protect against unauthorized access to the acquisition of personal information likely to result in a material risk of identity theft or other fraud for respective individuals.
- Encourages businesses to comply with established frameworks and gain an affirmative defense to tort actions arising from alleged "failure[s] to implement reasonable information security controls, resulting in a data breach."
- To qualify for safe harbor, businesses must "reasonably conform" with one of the eight commonplace industry-recognized frameworks, including HIPAA, GLBA, FISMA, and NIST's Cybersecurity Framework.

Existing Data Obligations – Record Destruction

- Most states require entities to destroy or dispose records reasonably (i.e. Georgia, South Carolina)
- These laws are often triggered when the sensitive or personally identifying information is no longer necessary for storage

Record Destruction – Ex: Florida

An entity or third-party agent must take reasonable measures to dispose of records containing sensitive personally identifying information within its custody or control when the records are no longer to be retained pursuant to applicable law, regulations, or business needs.

Fla. Stat. Ann. § 501.171

Existing Data Obligations – Prohibitions on SSN Use

Many states (including Georgia) have explicit prohibitions on how social security numbers can be used and sent

- Important to look at encryption methods
- Level of exposure in electronic and carrier mail
- Manner in which it is transported

Prohibitions on SSN Use – Ex: Hawaii

Entities should not

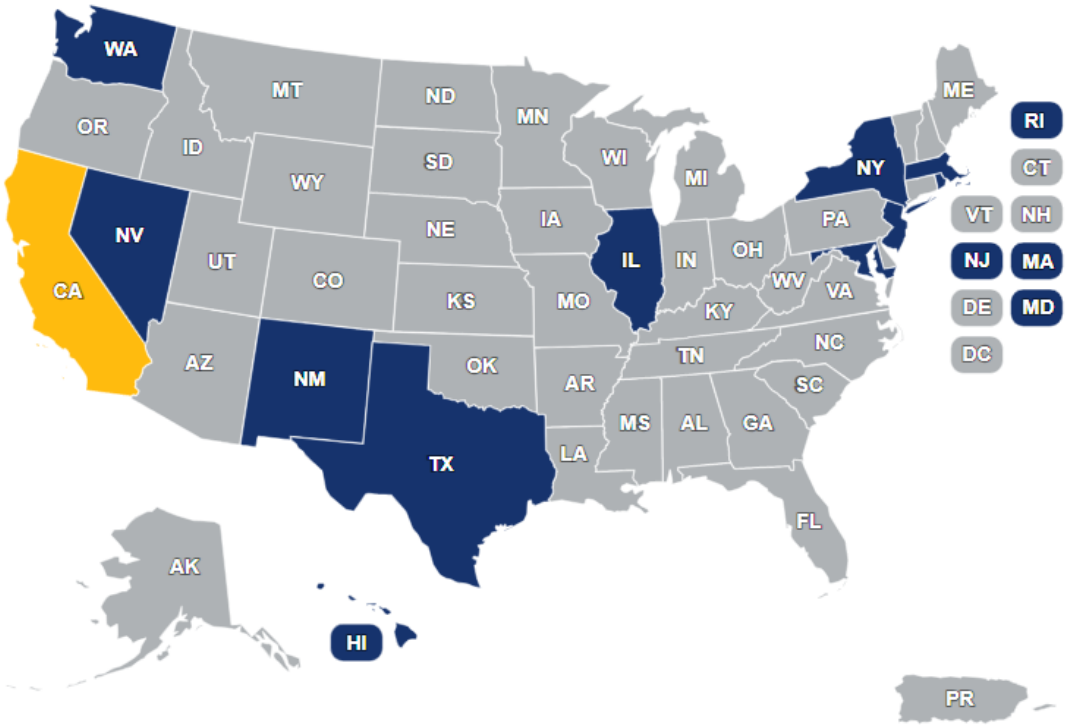
- Make SSN available to general public
- Print or embed entire SSN
- Require whole SSN be transmitted on internet through unsecured server
- Send exposed SSN through the mail

Haw. Rev. Stat. Ann. § 487J-2

Affirmative Data Obligations

Beyond Breaches: An Overview of Statutes, Regulations, and Legislation Affecting Business Obligations and Consumer Rights with Respect to Data

- **Hover over a state** to see introduced legislation or proposed regulations.
- **Click on a state** to see enacted statutes and adopted regulations.



Has the jurisdiction adopted an omnibus statute vesting residents with enumerated rights (e.g., the right to opt-out or the right to be forgotten)?

- Yes
- No*
- No, but an omnibus bill is being considered

*Even though there are no laws vesting residents with enumerated rights, companies may have other affirmative data obligations. Click on the state to see enacted laws; hover to see pending legislation

Last Updated: 5/15/19

StateDataUseLaw.com

Questions?

StateDataUseLaw.com

Phil Gura

T: 404-888-7480
E: Phil.Gura@WBD-US.com

Dominic Panakal

T: 404-879-2481
E: Dominic.Panakal@WBD-US.com

WOMBLE
BOND
DICKINSON