womblebonddickinson.com

WOMBLE BOND DICKINSON

What You Need to Know to Avoid Costly Lawsuits on Data Privacy, Cybersecurity, & Telecommunications

National Government Affairs Roundtable & Legal Symposium

July 31, 2019

Baker McKenzie.

Presented By

Panelists

- Artin Betpera, Womble Bond Dickinson (US) LLP
- Michael C. Egan, Baker McKenzie

Moderator

- Cathy A. Hinger, Womble Bond Dickinson (US) LLP

Areas Of Regulation

- **Data Privacy Laws**
  - European General Data Protection Regulation (GDPR) and Other Omnibus Data Protection Laws Outside of the U.S.
  - California Consumer Privacy Act (CCPA)
  - CCPA-Like Laws on the Horizon in the U.S.

- **Laws That Regulate Communications with Consumers**
  - Telephone Consumer Protect Act (TCPA): Calls/Texts

Do These Laws Apply To My Business?

Most likely.

- NAA Poll Results:
  - Consumer Data Privacy Laws
    - Almost all (83%) of responding members engage in regulated activities
    - Approximately 50% of survey responses revealed a potential compliance gaps
  - Telecommunication Laws
    - Nearly 100% of responding members engage in regulated activities
    - Approximately 50% of survey responses revealed potential compliance gaps

Data Privacy Laws Update

Scope of Data Privacy Laws

- Regulate the collection, use, storage, disclosure, and other processing of “personal data” or “personal information”

- Two approaches to regulation globally:
  - United States: Generally sector-specific (HIPAA/HITECH, GLBA/FCRA, and the like) and data-specific (SSNs, bank account, credit/debit card numbers), but shifting towards omnibus at the State Level (e.g., California)
  - European Union: Omnibus privacy laws applicable to all personal data, regardless of sector, category of individual, or type of personal data; EU tends to lead the rest of the non-US world

Personal Data

- **What is *personal data*?**
  - Any information relating to an identified or identifiable natural person
  - Such identification can be:
    - direct (e.g., by reference to the person's name); or
    - indirect (e.g., by reference to a unique number that relates only to them, such as an employee ID number).
  - Personal data can be a fact (e.g., phone number) or opinion (e.g., performance appraisal) and examples include the data subject's name, contact details (including business contact information), photograph, behavioral information, IP address, etc.
- **Certain categories of personal data are considered *sensitive personal data***
  - Must not collect or process sensitive personal data unless very specific conditions are met
  - Categories of personal data that are often considered sensitive personal data: race/ethnic origin, political opinions, union membership, genetic data, biometric data, health/medical data, sexual orientation, criminal convictions/offences, national or tax identification number

Notable global news in data privacy

1. European Union: General Data Protection Regulation ("GDPR")
2. Brazil: General Data Privacy Law
3. China: Cyber Security Law
4. Canada: Amendments to the Personal Information Protection and Electronic Documents Act
5. Global data security incidents and data breaches
6. Significant data use scandals

***Global trend*: More protection for consumers, more liability for companies**

***Business impact*: Certain social media companies have shifted their business models with respect to data sharing and companies have shifted to a new focus on privacy**

Meanwhile, in the United States…

1. All 50 states have enacted breach notification laws and some states have expanded the definition of "personal information" and certain states are implementing new or updating existing data security requirements
2. SEC has issued new rules regarding disclosure of cybersecurity events
3. FTC has announced its intent to update the Safeguards and Privacy rules under GLBA, most notably to require covered financial institutions to encrypt customer data
4. FTC's increased enforcement of privacy rules and regulations, including its largest settlement ever for privacy violations **($5 billion)**

Most notably, the California Consumer Privacy Act (CCPA), a law inspired by the GDPR, will become operational on January 1, 2020

Data Privacy Laws Update

California Consumer Privacy Act

California Consumer Privacy Act Overview

1. Most comprehensive “consumer” privacy rights law in the United States
2. Effective as of January 1, 2019, but operative January 1, 2020
3. Creates expansive definition of “personal information”
4. Creates new data privacy rights for California consumers, including rights to access, deletion, and opt-out of “sale” of personal information
5. Applies to companies worldwide, B2C and B2B
6. New statutory damages in case of data security breaches
7. Companies must ensure employees and individuals responsible for handling consumer inquiries receive training about the CCPA

Personal information – a broad term …

- Identifies, relates to, or describes …
- Capable of being associated with …
- Could reasonably be linked with …

Consumer

Household

Certain industry-specific types of data are not covered by CCPA

Consumers and covered businesses

Consumer

1. "**Consumer**" refers to residents of California (e.g., including employees, individual representatives of corporate customers).

2. In general, a person who stays in the state for other than a temporary or transitory purpose. Someone who resides in California for 6 months + 1 day.

Scope

Scope: Applies to businesses (and their parent co. / subsidiaries that share the same branding) doing business in California and:

- have annual gross revenues in excess of **$25 million**; or
- annually receive for a commercial purpose, alone or in combination, the PI of at least **50,000** or more California consumers, households, or devices; or
- derive **50%** or more of annual revenues from selling consumers' personal information.

Access and deletion rights

Access

- Business must comply within 45 days of receiving verifiable consumer request
- Disclose all relevant information with a 12-month ‘look-back’ period
- Types of information: categories of personal information, specific pieces of personal information, categories of sources, commercial purpose for collecting or selling personal information, categories of third parties personal information is shared with

Deletion

- Can request deletion of any personal information the business has collected from you
- Business must comply within 45 days of receiving verifiable consumer request
- Business does not need to delete if the personal information is necessary for certain purposes

"Sale" – another broad term…

- "Sale" refers to "the selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating . . . a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration."
- See also Consumer rights

Not a “Sale”

- Not a “**Sale”** of data when company discloses personal information:
- At consumer’s direction or intent to interact with third party, subject to additional conditions and limitations;
- To alert third party that consumer has submitted an opt out request for sale of their personal data
- As part of a merger, acquisition or bankruptcy or other transaction in which 3rd party assumes control of all or part of the business
- to service provider subject to conditions and limitations, including:
  - the company has provided sufficient notice to the consumer of this sharing; and
  - the personal information is used to for perform a business purpose for “**services that the service provider performs on the business’ behalf**” and the “service provider does not further collect, sell, or use the personal information except as necessary to perform the business purpose.”

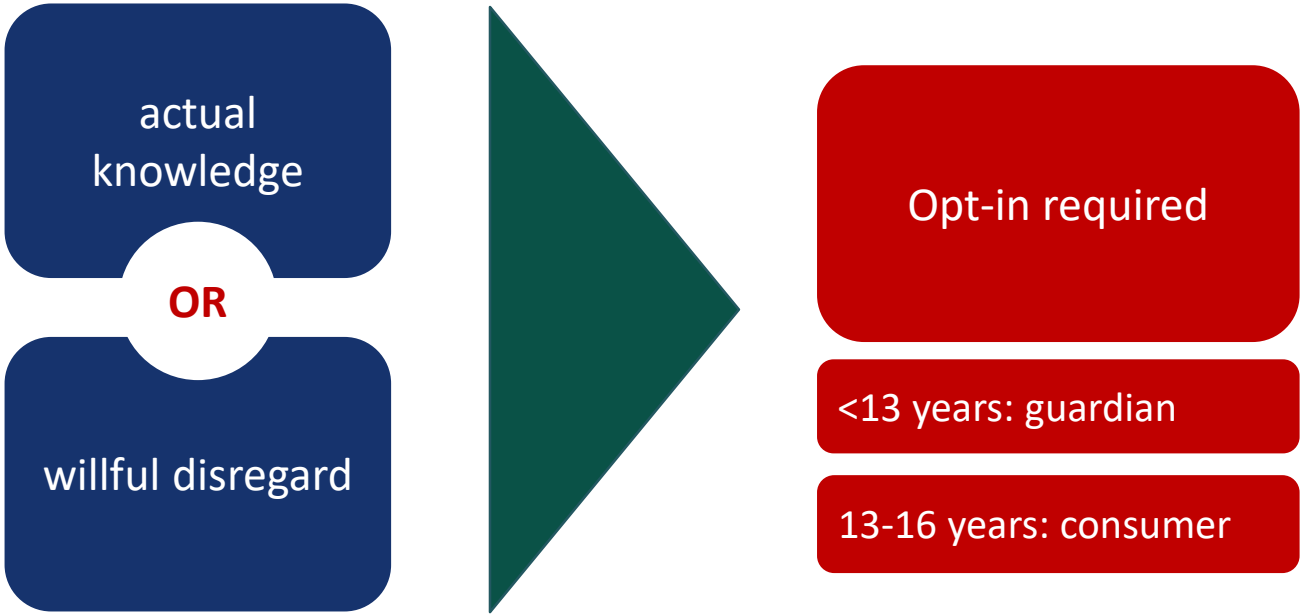
Right to opt out

- Consumer can direct the business not to sell consumer's personal information to a third party
- Business cannot request that a consumer authorize sale within 12 months of consumer exercising the right to opt out
- Third party cannot on-sell personal information unless consumer has notice and opportunity to opt out
- See also **Notice and disclosure** requirements

Minors' rights

Selling information of a minor

- Business cannot sell personal information of a minor without minor's opt-in consent



Non-discrimination

Right to equal service

To watch: How are these rights and restrictions intended to interact with each other?

Equal

Service

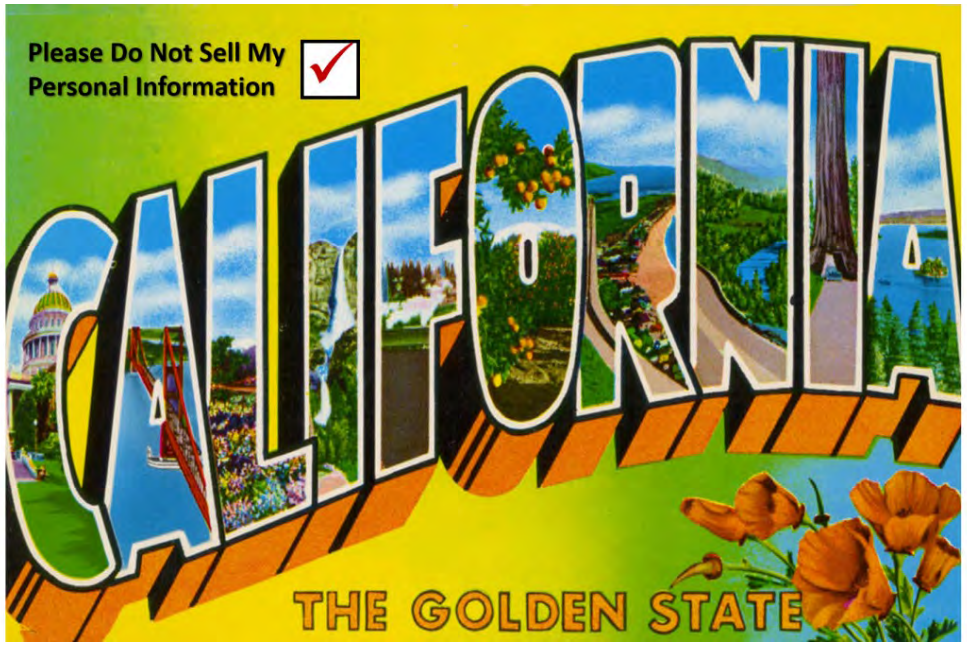
- No discrimination against consumer because of exercising CCPA rights
- Exception: if different price/quality is reasonably related to value provided to the consumer by consumer's data
- *Can* offer financial incentives for use of personal information

Privacy policy

Include the following information:

- Right to request deletion of personal information
- Categories of personal information collected, sold
- Specific pieces of personal information collected
- Categories of sources of personal information
- Categories of third parties personal information is shared with
- Commercial purpose for collecting or selling personal information
- Right to opt out of sale (if any) of personal information – link "**Do Not Sell My Personal Information**"

Do Not Sell My Information Link



- Website link ("Do Not Sell My Personal Information") to a web page to opt out
- Clear and conspicuous
- Must not require consumer to create an account to opt out

Sanctions

1. Enforcement: California Attorney General

a) Curing Period. Attorney General will provide an entity found to be in violation with written notice of the violation along with a 30-day period to cure before imposing fines.

b) Fines. $2,500 per violation if the company fails to cure or $7,500 for intentional violations.

2. Private right of action

a) Consumers have a limited private right of action in connection with:

- a breach of non-encrypted or non-redacted personal information (narrower definition in this context); and
- resulting from a violation of reasonable security practices and procedures.

b) Between $100 and $750 per incident or actual damages, whichever is greater.

c) Consumer must give the business 30 days prior notice before filing to allow the company to cure violation.

CCPA-like trends in the United States

State	Status	"Sale" same as CCPA?	Notice beyond CCPA?
Hawaii	Referred to Senate Committee on 1/24/2019	**Yes**	**No**
Illinois	Referred to Committee on Assignments on 3/28/2019	**Yes**	**No**
Maryland	Referred to Senate Finance Committee on 3/8/2019	**"Sale" not defined**	**No**
Massachusetts	Referred to Committee on Consumer Protection and Professional Licensure on 1/22/2019	**"Sale" not defined**	**No**
Nevada	Enacted; effective date October 1, 2019	**"Sale" not defined**	**No**
New Jersey	Referred to Senate Commerce Committee on 7/23/2018	**"Sale" not defined**	**No**
New York	Multiple Bills Referred to Senate Consumer Protection Committee (including one with "Data Fiduciary" concept)	**Varies by bill**	**No**
Pennsylvania	Referred to House Consumer Affairs Committee on 4/5/2019	**"Sale" not defined**	**No**
Rhode Island	On 4/30/2019, the Committee recommended this measure be held for further study	**Yes**	**No**
Washington	On 4/28/2019 by resolution, returned to Senate Rules Committee for third reading	**Yes**	**No**

CCPA Compliance activities

Steps to complete before January 1, 2020

Data Inventory

- Conduct inventory of consumer and employee/HR databases
  - Review consumer touchpoints and interfaces, including websites and social media, and digital marketing landscape
  - Identify data that is not subject to CCPA (e.g. HIPAA protected health information)
- Review third party data access and sharing and conduct data mapping exercises

Privacy Policy and Other Notices Management

- Update privacy notices to reference new consumer rights
- Update employee, job applicant and contractor privacy notices
- Have process for annual updates

"Do Not Sell" (DNS) Link Deployment

- Deploy DNS Web pages and links
- Have process for Opt-Out and Opt-In (age-based) management (including by 12 month non-solicitation)

Vendor Management

- Vendor Contract Negotiation
  - Update agreements to ensure compliance with CCPA consumer rights
  - Potential negotiations to avoid the definition of "sale" of consumer PI

Operational Processes

- Consumer PI asset inventory management and maintenance
- Consumer Right's Request process implementation
  - Consumer Rights' Request verification process (and honoring "Do not Sell" requests" and avoiding requesting additional consent for 12 months)
  - Toll free telephone number and website
- Incident management process
- Information Security compliance control management

Telephone Consumer Protection Act

Knowing When The Law Applies and
How to Form a Compliance Plan

What Is The TCPA?

- **The TCPA is a law passed in 1991 that regulates pre-recorded/artificial voice calls, calls using an automatic telephone dialing system (ATDS), and faxes.**

- **What are the risks?**
  - Extremely steep statutory penalties (between $500 and $1,500 per text/call) that add up extremely quickly and motivate plaintiff's lawyers to sue for violations.

How Do I Know If The TCPA Applies?

- **If your business calls, texts, or faxes, then the TCPA likely applies to some of your business practices.**

- **Do you:**
  - Use a dialing system (*i.e.* something other than a desk phone) to make calls to cell phones?
  - Use a text message platform/application to send out text messages?
  - Make calls using a pre-recorded or artificial voice?

How Do I Know If The TCPA Applies?

- **NAA Survey Results:**
  - Communications with tenants, prospective tenants, or other consumers via:
    - Text message – 75%
    - Pre-Recorded Messages – 20%
    - Fax – 25%
  - Text messaging is quickly becoming a dominant form of B2C communications.
- **Your text messages are very likely regulated by the TCPA.**

Text Messaging

- **NAA Survey - most common ways of sending text messages for business purposes:**
  - Smartphone;
  - Automated/web-based text platform.

- **Purpose for sending text messages - examples:**
  - Leasing/sales;
  - Rent collection;
  - “Concierge” services.



Text Messaging Ground Rules

Two fundamental rules:

1. **DO NOT** send a text message using an ATDS without consent; and

2. **DO NOT** send a text to a number registered on the National Do Not Call Registry for “telemarketing” or “advertising” purposes.

Rule #1 – ATDS Use

Am I using an ATDS?

- The law is in flux, so it depends.
- Compliance perspective: any type of technology-based solution that allows you to efficiently communicate with consumers should be treated as an ATDS.
  - Sends texts in batches;
  - Sends texts based on templates;
  - Sends texts to numbers on a list/database.

Rule #1 - Consent

- **Do I have consent to send the text?**
  - The answer depends on the nature of the message.
- **“Informational”**
  - Texts sent for non-marketing/promotional purposes, like maintenance notices/updates, package delivery notifications, collections, etc.
- **“Telemarketing” or “Advertising”**
  - Promoting the purchase, rental, or investment in a good or service (i.e. new lease/lease renewal promotions, texts about new units, etc.)

Consent For Informational Messages

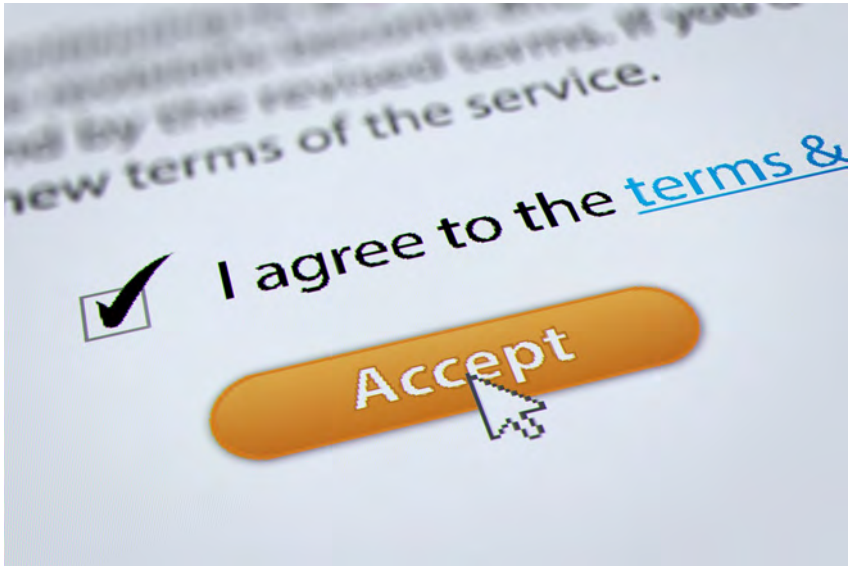
- **Informational Messages:** Prior Express Consent May Be Presumed.
  - Most common form: a consumer voluntarily provides a phone number to a business;
  - Can be obtained in other ways, such as written disclosure on an application, or in a lease agreement.

Consent For Marketing Messages

- **"Telemarketing" or "Advertising" Messages:** Prior Express Written Consent.
  - Written agreement, signed by the borrower specifically authorizing calls/texts for marketing purposes, and containing other conspicuous disclosures.
  - NAA Survey: About 50% of responding members call/text for marketing purposes.

Consent For Marketing Messages

- **“Capturing” Written Consent**
  - Old Fashioned Way: Consumer places their wet ink signature on a physical document containing the agreement;
  - Digital Way: Consent may also be obtained on a website via “clickwrap” type agreement;
- **Consent obtained via third party lead generator:**
  - Presents a whole new set of issues involving reliance on consent obtained by a third party.



Consent May Be Revoked

- The FCC and many courts have recognized that a consumer may revoke their consent by expressing a desire to no longer receive calls/texts.

- **Text Message Tip:**
  - Text messages should contain clear opt out instructions, *i.e.* “text STOP to stop”;
  - STOP requests should be immediately honored, and added to an internal DNC list.

Rule #2 – The DNC

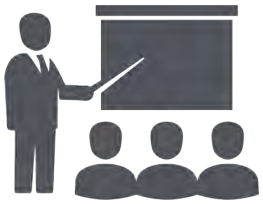
- **Am I texting/calling phone numbers for marketing purposes that are registered on the DNC? If so, do I have consent?**
- **Differences from Rule #1:**
  - Applies regardless of whether an ATDS is used;
  - Applies to both cell and landlines so long as the number is registered on the DNC.
- **Similarities to Rule #1:**
  - Same definition of “telemarketing” and “advertising” as Rule #1;
  - Same “prior express written consent” requirements apply.

Rule #2 – The DNC

- **Exception to consent rule: the "Established Business Relationship" (EBR)**
  - Prior express written consent not required if there is an EBR, which is either: (1) an inquiry from the consumer within the past (3) months; or (2) a transaction with the consumer within the past 18 months;
  - When would this be helpful?
    - Situations when you are texting/calling someone for marketing purposes manually (i.e. using your thumbs from a smartphone).

Rule #2 – The DNC

- **Additional technical requirements include:**
  - Written policy, available upon demand, for maintaining a do-not-call list;
  - Training of personnel engaged in text/telephone marketing;
  - Maintenance of a do-not-call list, and policy to honor do-not-call requests from consumers.



Developing Compliance Infrastructure

- **Have a written policy in place:**
  - Develop TCPA compliant protocols;
  - Ensure uniform application of those protocols in your operations;
  - They are required if you are calling numbers registered on the DNC for marketing purposes.

Developing Compliance Infrastructure

- **Recordkeeping**
  - Ensure you are keeping record of the source of all the telephone numbers you call/text, and consent you obtained to call/text that phone number;
  - Ensure you are keeping a record of all opt-out requests.
- **Consult with experienced counsel to help develop a bespoke compliance strategy based on your specific calling/texting operations.**

Want More Information?

Artin Betpera
Email: artin.betpera@wbd-us.com
Telephone: 657-266-1051

Michael C. Egan
michael.egan@bakermckenzie.com
Telephone: 202-452-7022

Cathy A. Hinger
Email: cathy.hinger@wbd-us.com
Telephone: 202-857-4489

Baker McKenzie.

WOMBLE BOND DICKINSON