

Compliance Update: California Consumer Privacy Act and Privacy & Data Security Hot Topics

Lead Generation World | Monday, January 20, 2020

Shannon K. Yavorsky, Partner

*Jonathan L. Pompan, Partner and Co-
Chair, Consumer Financial Services Practice Group*

*Rob Seaver, Executive Director,
LeadsCouncil, Moderator*

VENABLE LLP



Important Information

Views expressed are those of the speakers only, and do not represent the views of their organizations.

This presentation is for general informational purposes only and does not represent and is not intended to provide legal advice or opinion and should not be relied on as such. Legal advice can only be provided in response to specific fact situations.

This presentation does not represent any undertaking to keep recipients advised as to all or any relevant legal developments. ATTORNEY
ADVERTISING.

Our Panelists and Moderator



Jonathan L. Pompan, Partner
Venable LLP
202.344.4383
jlpompan@Venable.com

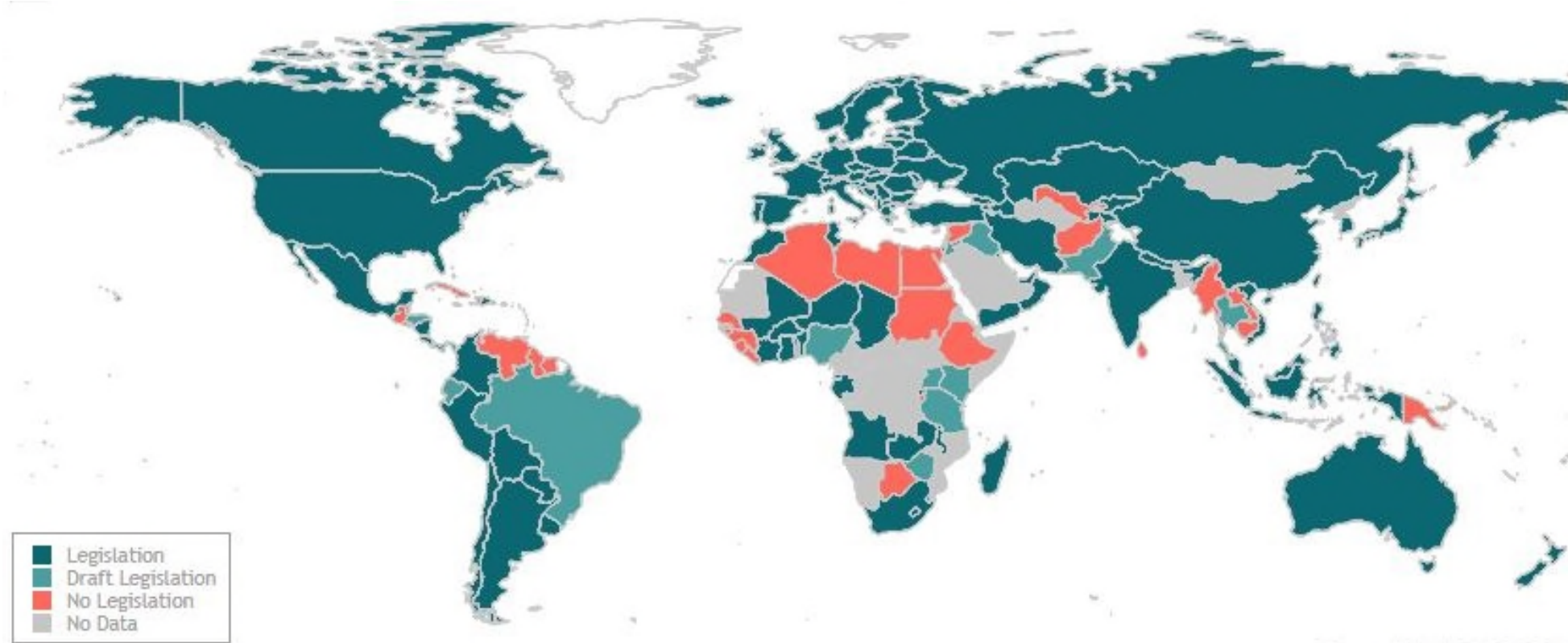


Shannon K. Yavorsky, Partner
Venable LLP
415.343.4486
skyavorsky@Venable.com



Rob Seaver, Executive Director
LeadsCouncil
202.695.5783
rob@leadscouncil.org

The Privacy Phenomenon (Global)



Source: UNCTAD, 27/03/2019

The Privacy Phenomenon (Global) *(c't'd)*

58%

Countries with **Legislation**

10%

Countries with
Draft Legislation

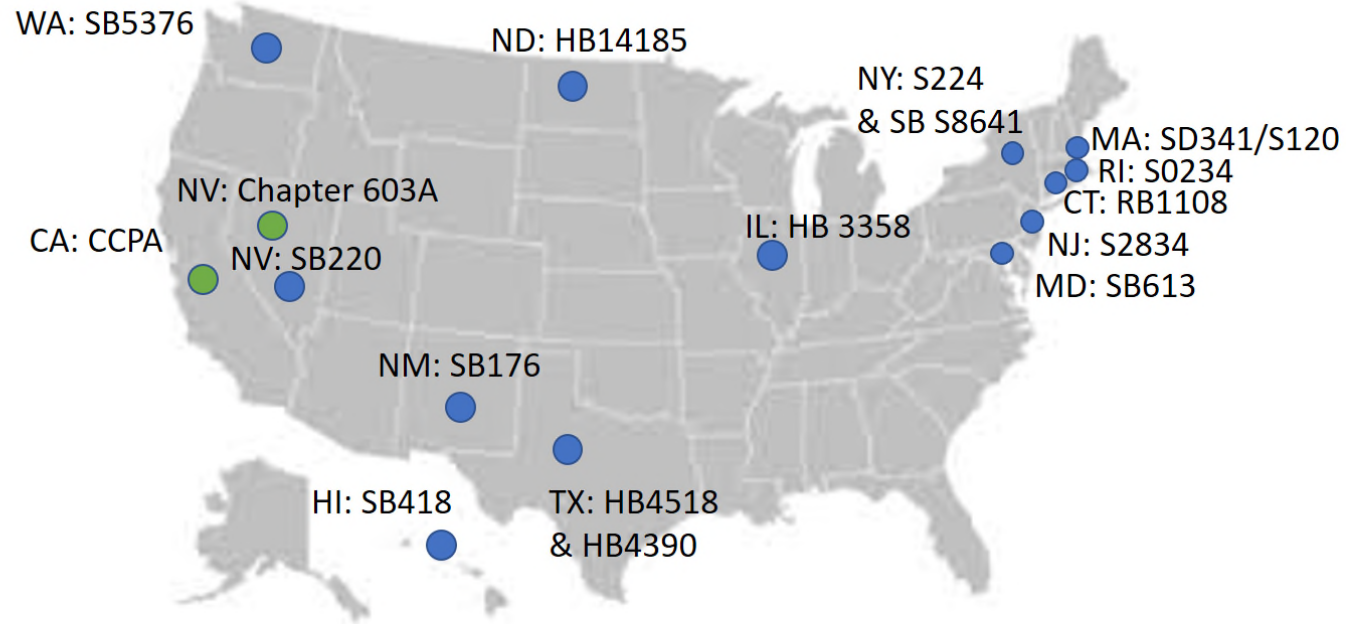
21%

Countries with
No Legislation

12%

Countries with
No Data

The Privacy Phenomenon (US)



- Law Passed
- Legislation Pending

Federal privacy laws:
HIPPA, GLBA, COPPA, ECPA, etc.

Making Sense of it All....



What we've learned from California's Consumer Privacy Act so far

BY ERIC GOLDMAN, OPINION CONTRIBUTOR — 01/11/20 02:00 PM EST
THE VIEWS EXPRESSED BY CONTRIBUTORS ARE THEIR OWN AND NOT THE VIEW OF THE HILL

81 COMMENTS



VENABLE LLP

Vox

CCPA, California's new privacy law, explained

What is CCPA? The California Consumer Privacy Act gives Californians some control over their data, but only if they know how to take ...

2 weeks ago



California Consumer Privacy Act (CCPA) FACT SHEET

The California Consumer Privacy Act (CCPA) was enacted in 2018 and takes effect on January 1, 2020. This landmark piece of legislation secures new privacy rights for California consumers. On October 10, 2019, Attorney General Xavier Becerra released draft regulations under the CCPA for public comment.

The CCPA grants new rights to California consumers

- The **right to know** what personal information is collected, used, shared or sold, both as to the categories and specific pieces of personal information;
- The **right to delete** personal information held by businesses and by extension, a business's service provider;
- The **right to opt-out** of sale of personal information. Consumers are able to direct a business that sells personal information to stop selling that information. Children under the age of 16 must provide opt in

The Verge

No one is ready for California's new consumer privacy law

Just like the GDPR, it's not totally clear what it means to be compliant with the CCPA.

2 weeks ago



Today's Session

- CCPA
 - Background and Scope of the CCPA
 - Consumer Rights & Requirements for Businesses and Service Providers
 - Draft CCPA Regulations
 - Enforcement and Legal Risks
- Related Topics
- Questions

Question

- **How many of you:**
 - **are in compliance with GDPR?**
 - **are in compliance with CCPA?**

Scope of the CCPA

Any company that does business in California and meets one or more of these standards:

Annual gross revenue of more than \$25 million

Collects or shares personal information annually from 50,000 consumers, households or devices

Derives at least 50% of annual revenue from sale of personal information

Obligations and limitations extend to all **personal information** maintained about **consumers**:

Consumer = any natural person who is a California resident

Personal Information = information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked with consumer or household ("PI")

Service Providers and Third Parties

Service Provider = a legal entity that is organized or operated for the profit or financial benefit of its owners, that processes information on behalf of a business and to which the business discloses a consumer's PI for a business purpose pursuant to a written contract, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the PI for any purpose other than for the specific purpose of performing the services specified in the contract.

Third party = a person who is not (1) the business that collects PI from consumers; (2) a person to whom the business discloses PI for a business purpose pursuant to a written contract.

Affiliates

Affiliates can be part of a single “business” only if:

- An affiliate “controls or is controlled by” the business **and**
- Shares common branding with the business
 - “Common branding” means a shared name, servicemark, or trademark

Affiliates within a single business:

- Can share personal information without providing an opt-out
- **BUT** access and deletion requests will apply across the business

Scope of Personal Information

Definition of Personal Information

- Information that:
 - Identifies, relates to, describes,
 - Is reasonably capable of being associated with, or
 - Could reasonably be linked, directly or indirectly,
 - With a particular consumer or household

Selected Examples (that are personal information if they meet the functional definition)

- Identifiers including name, postal address, online identifier, IP address
- Unique, persistent identifier to recognize a device linked to a consumer or family, over time and across services, including cookies, customer number, unique pseudonym, and other persistent or probabilistic identifiers
- Geolocation data
- Internet and other network activity information, including browsing, search, and usage data

General Exceptions

General exceptions to the CCPA include activities required to:

Comply with federal, state, or local laws

Comply with civil, criminal, or regulatory investigation

Cooperate with law enforcement

Exercise or defend legal claims

The CCPA also does not apply to:

Personal information that is aggregated or de-identified

Publicly available information

Information covered by GLBA, CalFIPA and the FCRA

Temporary Exceptions: HR data and B2B data

Until January 1, 2021, most portions of the CCPA do not apply to certain HR and B2B data.

- Many of the CCPA's requirements will not apply to personal information collected about **job applicants and employees** so long as that information is used solely within that person's role or former role with respect to the business. Businesses are still required to inform consumers of the categories of personal information collected and the purposes for which those categories are used.
- Still need to provide opt-out for business contacts.
- Private right of action still applies.

Key Requirements

- Consumer right to request certain information about practices, and ***specific pieces of personal information***
- Consumer right to request deletion of personal information, with some exceptions
- Consumer right to opt out of “sales” of personal information
 - “Do Not Sell My Personal Information” link and webpage
- Verification of consumer requests
 - Specific categories of personal information
 - Specific pieces of personal information
- Training for businesses handling CCPA requests and record keeping of CCPA requests
- Implementation requirements

Consumer Rights: Access and Deletion

- **Access:** Consumers can request categories and specific pieces of personal information collected, as well as sources of data and third parties that companies shares data with (*i.e.*, “sales”). Typical timeline is 45 days to respond.
- **Deletion:** Consumers can request that companies delete personal information collected from them, with some exceptions.
- Companies may be able to leverage EU tools to meet CCPA obligations



Draft Regulations

- On October 10, 2019, California Attorney General Xavier Becerra issued Draft Regulations implementing the CCPA.
- The Draft Regulations are subject to a public comment period and public hearings that will close on December 6, 2019, after which they may undergo further revisions before becoming enforceable in 2020.
- The Draft Regulations contain some clarifications, and include some additional obligations beyond the CCPA's current requirements.

Draft Regulations (Cont'd)

- **Among other key aspects**, the proposed CCPA regulations include that:
 - Businesses must make available **two or more methods to opt-out** of the sale of PI, including, at a minimum, an interactive webform accessible via a link titled “Do Not Sell My Personal Information” or “Do Not Sell My Info” and a method that reflects how the business primarily interacts with consumers.
 - Businesses must act on opt-out requests **no later than 15 days** from the date of receipt of the request.
 - All businesses must establish, document, and comply with a **reasonable method for verification**, which may include the use of a third-party verification system.
 - Businesses may require **authorized agents** used by consumers to submit requests to know or delete to be provided with written permission to do so. Businesses may require that consumers verify their identity directly with the business.
 - A financial incentive is a **discriminatory practice** if a business treats a consumer differently for exercising a right conferred by the CCPA. However, a business may offer a price or service difference if it is reasonably related to the value provided to the business by the consumer’s data.

CCPA Enforcement and Penalties

California Attorney General Enforcement

- The California Attorney General may bring suit against a business to enjoin any conduct that violates a provision of the CCPA or obtain **civil penalties of \$2,500 per violation or \$7,500 for each intentional violation.**
- **30-day cure period applies.**

Private Right of Action

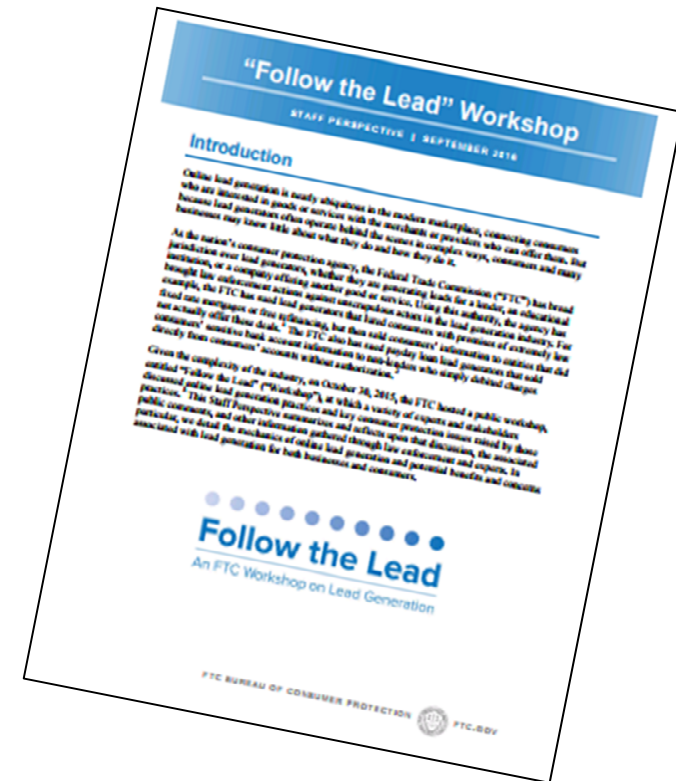
- Any consumer whose nonencrypted and nonredacted PI is subject to unauthorized access, exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PI may institute a civil action for:
 - Injunctive relief, any other relief the court deems proper; and/or the **greater** of damages in the amount of **\$100 - \$750 per consumer per incident or actual damages.**
- **30-day cure period applies.**

Key Takeaways

- Businesses should consider whether they are “selling” personal information.
- Businesses should remain aware of obligations under the CCPA that require action by the enforcement date as well as exemptions that apply to their business.
- Businesses remain abreast of CCPA news that will help their business adapt efficiently to the new landscape as the CCPA and the Regulations are finalized.
- Businesses should consider building a scalable privacy program based on established privacy principles.

FTC Focus on Lead Generation Privacy and Data Security through FTC Act (UDAP), Telemarketing Sales Rule, and GLBA

- Disclose clearly to consumers who you are and how you will share their information.
- Monitor lead sources for deceptive claims and other warning signs like complaints.
- Vet lead buyers and avoid selling remnant leads to buyers with no legitimate need for sensitive data.
- Keep sensitive data secure.
- GLBA Rulemaking to add “Finders” to Scope of Privacy and Safeguards Rules



FTC Focus on Deceptive Claims To Consumers

- Who can be held liable
 - ✓ Publisher
 - ✓ Affiliate Network
 - ✓ Service Provider

(FTC v. LeanSpa, FTC v. Inbound Call Experts, FTC v. Five Star Auto)

- Who is making the offer
(FTC v. Mallett)
- What is being offered
(FTC v. Expand, US v. Consumer Education.info)
- Security of Consumers' Personal Data
(FTC v. ValueClick)
- How data would be used
(FTC v. Blue Global)

“Lessons” for Users of Leads From Lead Generators

According to the FTC Director of Consumer Protection the five “lessons” for users of leads from lead generators are:

1. Exercise Due Diligence
2. Establish Contractual Requirements and Service-Level Standards for Compliance and Performance
3. Reserve Audit Rights
4. Monitor Vendors and Take Action; and
5. Require Vendors to Maintain Same Standards with Subcontractors

How will sellers meet these requirements if implemented by buyers?

What's Generating FTC Enforcement Actions?: A Continued Focus on Lead Generation and Telemarketing

Recent Example:


- Allegations:
 - Falsely representing affiliation with military
 - False representations on sharing of data and contact information
 - Do Not Call Registry Telemarketing
 - False representations of endorsement by military, independent advisor, or employer
- Impact:
 - \$30m in consumer redress
 - System to review all materials
 - Prohibition on misrepresentations about benefits of product and services

Additional Examples:

- Customer review fraud
 - Attempts to drive positive results and no disclosure of material connections in endorsements and reviews
- Influencer campaigns

Note: Strong internal push for stronger settlements

FTC Staff Public Encouragement of Best Practices



Portfolio Media, Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

FTC To Crack Down On Cos. That Buy Data From Scammers

By Alison Noon

Law360 (May 15, 2019, 10:24 PM EDT) -- A high-ranking official at the Federal Trade Commission said Wednesday that the agency is cracking down on companies that purchase consumer data gathered through online scams, funding what he called an ecosystem of deceit on the internet.

Andrew Smith, director of the FTC's Bureau of Consumer Protection, said at a compliance conference in New York that companies using data to target advertisements at certain consumers need to ensure that that data was gathered with every relevant legal consent. The FTC, he said, is coming for those who don't.


Smith said the agency is targeting advertisers, one of many levels in the affiliate marketing business, believed to be bankrolling people who collect consumer data through less-than-honest means, then sell it to organizations consumers didn't authorize. The data is most often used to increase the likelihood that an advertisement will be clicked, resulting in what Smith called "bad traffic."

"We're not just looking at the people who generate bad traffic, but looking at the people who purchase that bad traffic," Smith said at the Comply 2019 conference hosted by regulatory technology firm PerformLine Inc. "You're going to see cases more frequently against advertisers in particular."

The cycle starts with bogus product pages, fake news websites and clickbait, Smith said, such as a banner on a web page that says "See what Honey Boo Boo looks like now."

"You click on it and then it says '\$50 gift card for answering some questions,' and the \$50 gift card never really materializes," Smith said. "But, before you know it, you've just answered a bunch of questions about whether you own your own home, whether you are interested in saving money on your energy bill, whether you are interested in a college degree, that kind of stuff."

When consumer data is developed using deceptive practices, Smith said, using it can cause for FTC litigation, too.



News, cases, companies, firms

Advanced Search


CONSUMER PROTECTION | CYBERSECURITY & PRIVACY | LEGAL INDUSTRY | EXPERT ANALYSIS | IN-DEPTH | TAX AUTHORITY | LAW360 UK | SEE ALL 61 SECTIONS

Expert Analysis - Opinion

Companies Must Manage Lead Generators Responsibly

By Andrew Smith

Law360 (September 25, 2019, 4:44 PM EDT) -- Successful manufacturers make supply chain management a top priority – asking questions about the source of raw materials they buy, building product specs into their contracts, reserving audit rights, exercising oversight authority, and insisting that vendors hold subcontractors to the same high standards. Recent law enforcement actions involving the lead generation industry show that advertisers should consider similar standards when the raw materials they buy are consumer leads.



Andrew Smith

Consumer Financial Protection Bureau: Technical and UDAAP

- Supervisory exams and nonpublic investigations continue to focus on advertising and marketing practices
 - Consumer Financial Protection Act (“UDAAP”)
 - Telemarketing Sales Rule
 - GLBA Privacy Rule
 - Substantive Consumer Financial Law (e.g., TILA)
- Interest in “bait advertising,” affiliate marketing, facial claims regarding products and services
 - Verticals in focus: debt relief services, tax debt relief, credit repair, mortgage advertising and practices, credit card marketing, lump sum payments for military pensions, student loans

Resources available at Venable.com

VENABLE LLP

The California Consumer Privacy Act of 2018
July 16, 2018
Tara Sugiyama Pitsochiv, Julia Kermochan Tama and Rob Harwell

On June 28, 2018, the California governor signed into law AB 375, which will come into force as the California Consumer Privacy Act of 2018 (CCPA) on January 1, 2020. The CCPA was passed by the California legislature in exchange for the withdrawal of a ballot initiative that had proposed a different consumer privacy law that was viewed as more onerous by many in the industry. The CCPA will cover companies doing business in California that collect personal information from California residents and meet certain thresholds related to company revenue or amount of data. For companies subject to the CCPA, the law is likely to compel significant changes in business practices at a time when many are still grappling with the impact of the EU General Data Protection Regulation. Among other significant elements, the CCPA applies to a broad range of information that relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. The CCPA creates new rights for consumers with respect to their data, including rights related to data access, data deletion, and opting out of the sharing or selling of personal information to third parties. The new law will be enforced by the California Attorney General, as well as through a private right of action when personal information is subject to unauthorized access and exfiltration, theft, or disclosure.

One exception to the CCPA relevant to the financial services industry is that the CCPA will not apply to the sale of personal information to or from a consumer reporting agency if the information will be reported in, or used to generate, a consumer report to be used in accordance with the Fair Credit Reporting Act. Additionally, the CCPA will not apply to personal information that is collected, processed, sold, or disclosed pursuant to the Gramm-Leach-Bliley Act ("GLBA") if the CCPA is in conflict with the GLBA. Please contact us for more information.

© 2018 Venable LLP. This document is prepared by the law firm Venable LLP. It is not intended to provide legal advice or create an attorney-client relationship. Each office may have its own electronic media, and this document may be stored on those media. It is not intended to be distributed outside the office.

VENABLE LLP

Lead Generation Advertising Compliance "Lessons"
October 17, 2019
Jonathan L. Pompan

Law enforcement, workshops, and reports from the Federal Trade Commission (FTC) have yielded five "lessons" for lead generation advertisers, according to an article that was published last month in *Law360* by Andrew Smith, director of the FTC Bureau of Consumer Protection. In it, he suggests that companies that purchase lead generation advertising must manage lead generators responsibly; just like manufacturers that make supply chain management a top priority.

The article draws attention from members of the lead generation advertising sector and their lawyers and compliance departments. Some commentators called it a tutorial on how to reduce risk in using lead generation advertising. For others the article was a cautionary tale of recent enforcement actions taken against a lawyer of lead generation advertising and the lead generators spotlighted in the article. In any event, the article was certainly reflective of the FTC's work in the lead generation area and reminder of the importance of legal compliance in the lead generation ecosystem.

According to Smith, "The complexity of the lead generation ecosystem isn't a shield against liability, nor does it exempt you from honoring fundamental consumer protection principles. Advertisers should take the lead in ensuring the leads they use weren't the product of deception."

The article highlights lessons from a recent series of cases that allege deceptive marketing, including the first time the FTC has held an education company liable for the tactics of lead generators under the FTC Act and Telemarketing Sales Rule (TSR).

As alleged by the FTC, an education company used sales leads from lead generators that falsely told consumers they were affiliated with the U.S. military, and that used other unlawful tactics to generate leads. The company's lead generators also allegedly induced consumers to submit their information under the guise of providing job or benefits assistance. The FTC also alleged that the lead generators falsely told consumers that their information would not be shared, and that both the education company and its lead generators illegally called consumers registered on the National Do Not Call (DNC) Register. The education company agreed to a settlement with conduct prohibitions and a \$30 million penalty.

The five "lessons" for users of leads from lead generators are:

1. Exercise Due Diligence
2. Establish Contractual Requirements and Service-Level Standards for Compliance and Performance

© 2019 Venable LLP. This document is prepared by the law firm Venable LLP. It is not intended to provide legal advice or create an attorney-client relationship. Each office may have its own electronic media, and this document may be stored on those media. It is not intended to be distributed outside the office.

VENABLE LLP

California Consumer Privacy Act Compliance Checklist: 10 Steps to Start Now
September 26, 2019
Shant P. Singh, Emilio W. Civitanes, Michael A. Signorelli, Julia Kermochan Tama, Kelly DeMarchis Buttle, Shannon K. Yavorsky, Tara Sugiyama Pitsochiv and Jami Mills Vlodav

Any company that collects data about California residents should start evaluating whether it is subject to new obligations and liabilities under the California Consumer Privacy Act (CCPA). Even businesses that meet the requirements of the EU General Data Protection Regulation (GDPR) will have more to do to prepare for the CCPA.

The CCPA will become operative on January 1, 2020. Enforcement by the California Attorney General can begin on July 1, 2020, or sooner if regulations are issued speedily. A "look back" period of 12 months for certain obligations, notably when responding to consumer requests for information, means that businesses should begin preparing for the CCPA much earlier. Below are 10 key tasks to get your business started now on the path to CCPA compliance.

1. Check whether the CCPA applies to your business. The CCPA generally will apply to businesses: (a) with over \$25 million in annual gross revenues; (b) that receive or share personal information for 50,000 or more consumers, households or devices; or (c) that derive more than half of their annual revenues from consumer data sales. But, even if your business falls into one of these categories, there are exemptions that may apply.
2. Inventory the personal data your business collects. Taking stock of your data collection will help determine how you apply the CCPA's new requirements. The CCPA covers a broader range of personal information than most U.S. privacy laws—among other things, it reaches any information that is capable of being associated with a consumer or household. As examples, IP addresses and other online identifiers, purchase history, browsing or search history, and inferences about a consumer can all be covered.
3. Prepare to execute access and deletion requests. The CCPA grants sweeping new consumer rights over personal information—such as access and deletion upon request. Your business's ability to respond to these requests will depend on being able to locate personal information maintained across systems. Your business will also need to navigate a variety of operational issues, such as verifying the identity of the consumer making the request, and assessing what exceptions will be available to your business.
4. Assess how you are sending personal information to other entities. Under the CCPA, businesses must allow consumers to opt-out of "sales" of their personal information and also inform consumers on request about sales and certain other disclosures. Any transfer of personal

© 2019 Venable LLP. This document is prepared by the law firm Venable LLP. It is not intended to provide legal advice or create an attorney-client relationship. Each office may have its own electronic media, and this document may be stored on those media. It is not intended to be distributed outside the office.

Cybersecurity and Privacy: A Survey of the GDPR and CCPA
July 2019

Ari Schwartz | Venable LLP
Timothy Yim | Imperva
Adriana Beach | 23andMe
Shannon Yavorsky | Venable LLP

VENABLE LLP

Generating Leads Legally: Regulatory and Litigation Quick Hits
Thursday, March 28, 2019, 2 pm – 3 pm ET

Daniel S. Blynn
DSBlynn@Venable.com

Alexandra Megaris
AMegaris@Venable.com

Stephen R. Freeland
SRFreeland@Venable.com

Jonathan L. Pompan
JLPompan@Venable.com

VENABLE LLP

LeadsCouncil



LeadsCouncil Information and Membership @ LeadsCouncil.com

The screenshot displays the LeadsCouncil website interface. At the top, the LeadsCouncil logo is on the left, and navigation links for 'Contact Us', 'Sign In', and 'Register' are on the right, along with social media icons for LinkedIn, Twitter, and RSS. A blue navigation bar contains links for 'Home', 'Membership', 'About Us', 'LeadsCouncil Standards', '2018 Leader Awards', and 'Complaints Comments & Suggestions'. The main banner features the word 'Compliance' in large white text, followed by a paragraph: 'LeadsCouncil's mission is to maintain a trusted association of vendors, buyers and sellers adhering to industry best practices. We promote and protect the growth of performance marketing through establishing and managing the ethical standards and guidelines regarding online performance marketing through self-regulation, education and government/association advocacy, lobbying on behalf of these members.' Below this text are two buttons: 'Learn More' (blue) and 'Membership' (green). On the right side of the banner, a white login form is overlaid, containing fields for 'Username or Email Address' and 'Password', a 'Remember Me' checkbox, a blue 'Log In' button, and a 'Lost Password?' link. A vertical 'Feedback' button is on the far right. Below the banner, a section titled 'Our Platinum Level Members' displays logos for 'IndustryAlerts', 'sparkroom', 'doublePOSITIVE Marketing Group, Inc.', and 'Velocify'. A blue pop-up box in the bottom left corner promotes the 'IndustryAlerts Newsletter' with a 'Subscribe now' button.

More Questions for Our Panelists?



Jonathan L. Pompan, Partner
Venable LLP
202.344.4383
jlpompan@Venable.com



Shannon K. Yavorsky, Partner
Venable LLP
415.343.4486
skyavorsky@Venable.com



Rob Seaver, Executive Director
LeadsCouncil
202.695.5783
rob@leadscouncil.org



© 2020 Venable LLP.

This document is published by the law firm Venable LLP. It is not intended to provide legal advice or opinion. Such advice may only be given when related to specific fact situations that Venable has accepted an engagement as counsel to address.

VENABLE LLP