Contra Costa County Bar Association

2022 MCLE SPECTACULAR

Building Our Future

CCCBA's Intellectual Property and Business Law Sections proudly present…

#4 PRIVACY AND INTELLECTUAL PROPERTY AND BUSINESSES - OH MY !

Leopold Lueddemann,
Law Office of Leopold Lueddemann; Brothers Smith

Ashley Shively,
Holland & Knight LLP

AGENDA

This course tackles the most important privacy- and security-related trends affecting businesses as well as upcoming changes to keep an eye out for.

Practitioners with be provided with the tools to issue spot key data privacy and security, and consumer protection concerns that frequently arise for clients. It will also cover updates on state and federal legislation and rulemaking.

Contra Costa County
Bar Association

2022 MCLE SPECTACULAR

Building Our Future

PROGRAM MATERIALS

Privacy and Intellectual Property and Businesses

Oh My!

Contra Costa County Bar Association
MCLE Spectacular
November 18, 2022
Morning Breakout Session, 11:00 am – 12:30 pm

Ashley Shively
Partner, Holland & Knight

Lee Lueddemann
Owner, Law Office of Leopold Lueddemann

Introductions

Lee Lueddemann
Law Office of Leopold Lueddemann
lee@lueddemannlaw.com

Ashley Shively
Holland & Knight LLP
Ashley.Shively@hklaw.com

Privacy level-setting

- Federal
  - Focus is on industries and sensitive data
- State laws
  - Patchwork of state privacy, consumer protection, and false advertising laws
- Considerations for businesses with global footprint
- On the horizon in 2023
- How do you apply this to clients
- Things to look out for
- Questions

Federal privacy laws focus on sensitive data

Special industry considerations	Health care (HIPAA)
	Financial services (GLBA, FCRA)
	Education (FERPA)
	Children (COPPA)
	FTC

A patchwork of laws at the state-level

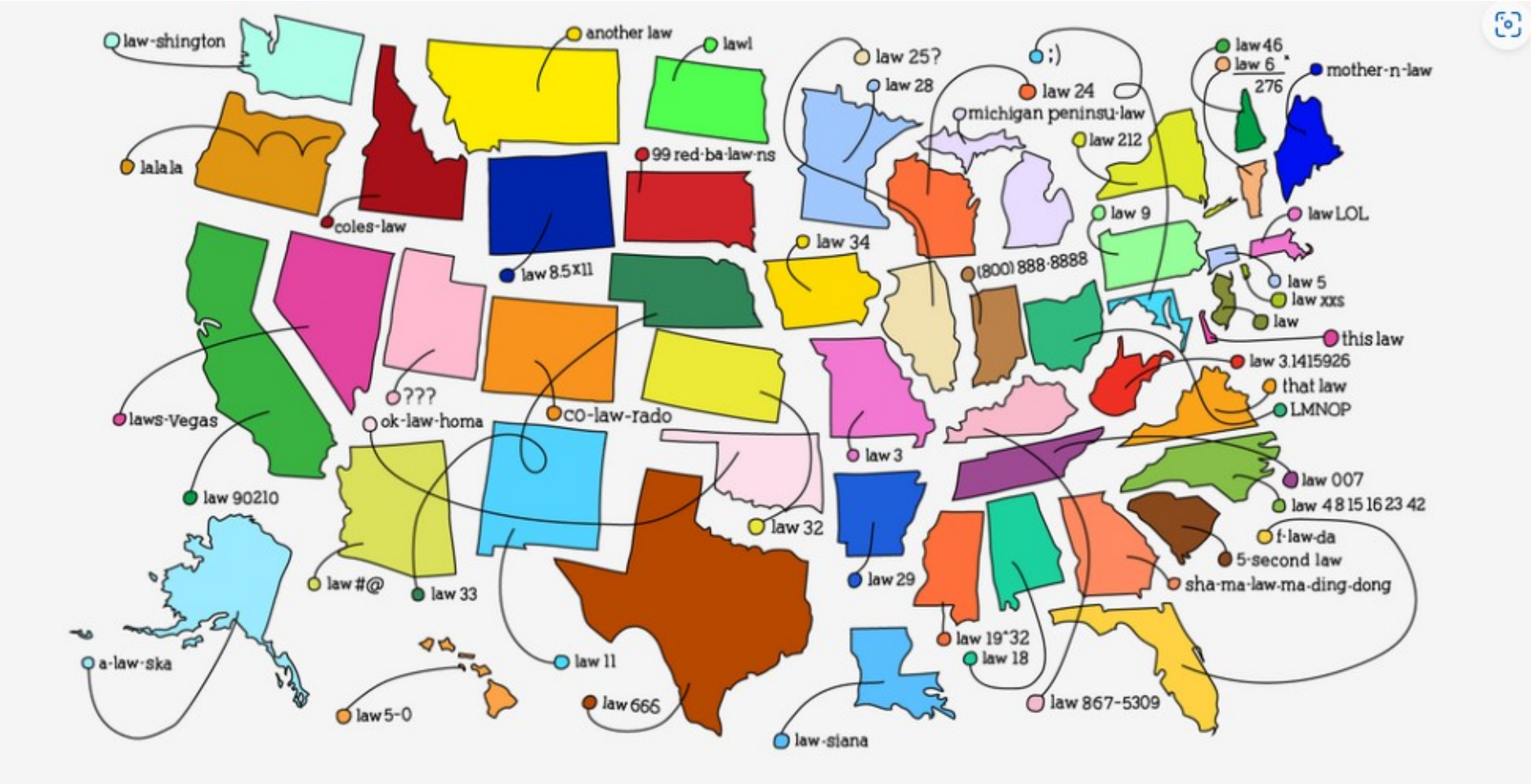
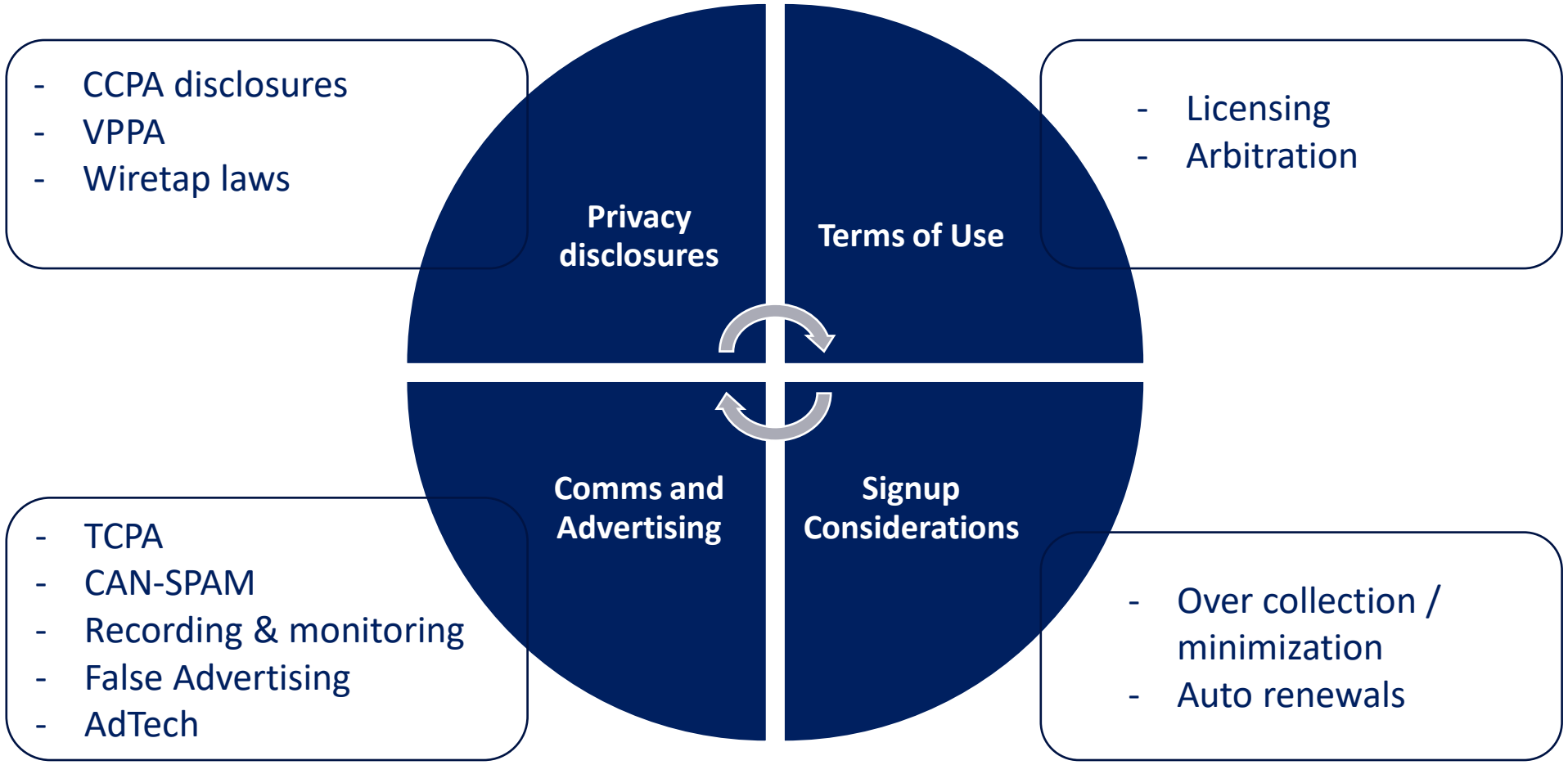


Illustration: Dana Davis

Consumer / Retail – Hot Topics



Consent and Transparency

- Let's talk about what these mean and why it is valuable for you and your clients.
- Threat = Risk x Vulnerability
- User-centric – Privacy by design.
  - Proactive and preventative commitment
  - It is the default. Specify use, minimization, limitation, and retention.
  - Embedded into design. Tech, audits, threat analysis.
  - End-to-end security. Lifestyle Protection.
  - Visibility and transparency. Accountability, Openness, Compliance.
  - Respect for User Privacy.

Data governance considerations

Data collection

- What do you <u>really</u> need (minimization)

Data use

Access

Storage, retention, and deletion

Purpose and use limitations

Disclosure

Monetization

A Brief History of CCPA

2018 – CCPA Enacted

- GDPR implemented one month earlier; all EU residents are covered data subjects
- “Consumer" broadly defined to include any California resident – not limited to individuals acting as consumers of goods and services for personal or household use.
- Effective 1/1/2020

2019 – Workforce and B2B exemptions added for 1 year

- In October, amendment passes that gives brief reprieve on compliance where PI is collected related to individuals acting in an employment capacity or as representative of a business
- But, Notice at Collection still required for workforce, and data breach cause of action still applies to workforce data

2020 – CPRA Passes

- Extends exemption for worforce and B2B until 1/1/2023

2022 – Full Steam Ahead

- Despite proposals, Legislative Session ended in August with no extension of exemptions

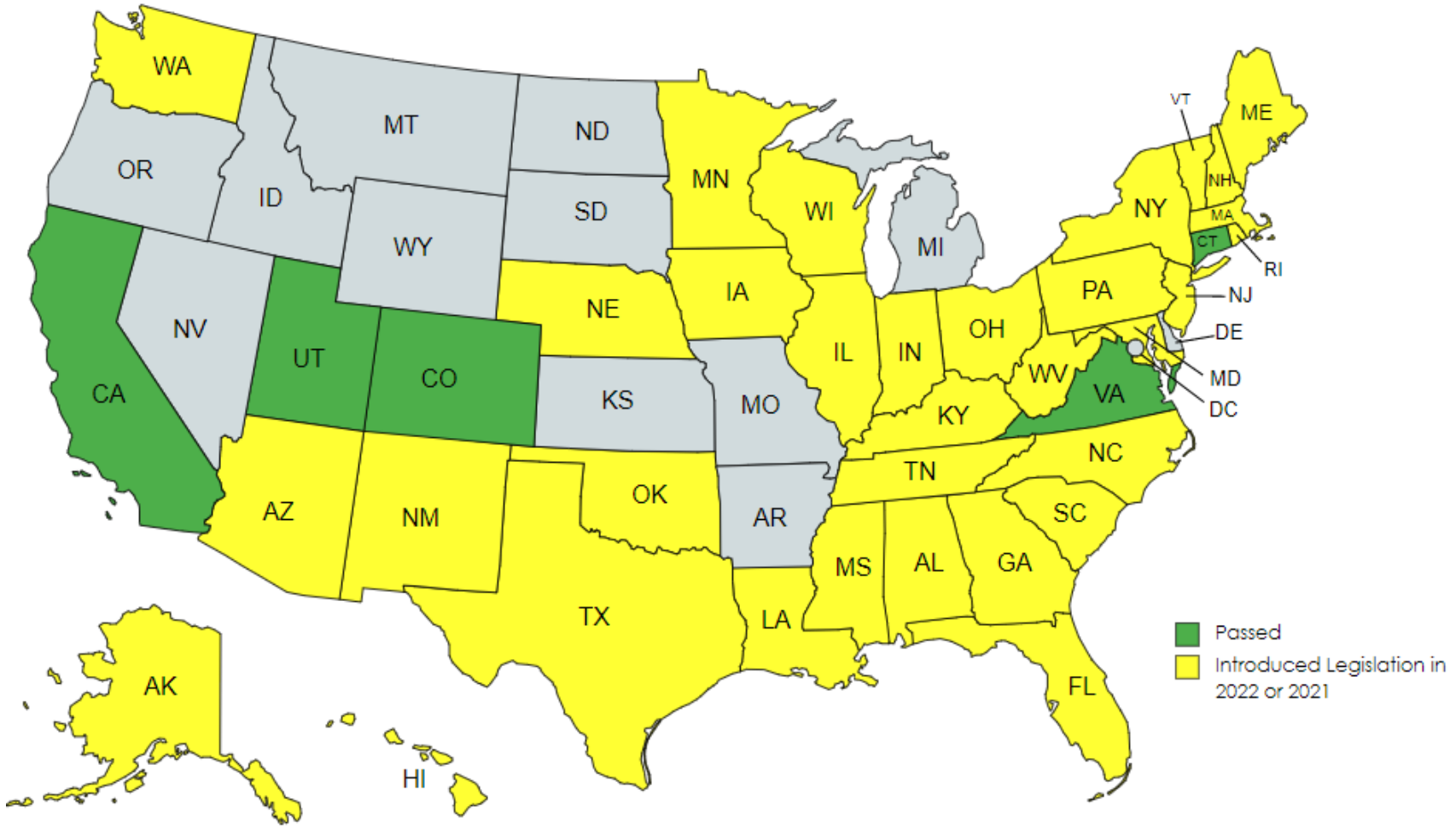
Breaking Down the New State Privacy Laws

Overview					
	California	Virginia	Colorado	Utah	Connecticut
Effective	California Privacy Rights Act (CPRA) fully effective Jan. 1, 2023	Jan. 1, 2023	July 1, 2023	Dec. 31, 2023	July 1, 2023
Private Right of Action	✓ Data breach only	✗	✗	✗	✗
Notice At/Before Collection	✓	✓	✓	✓	✓
Opt-In Default for Sensitive Personal Information (SPI)	✗ Opt-out	✓	✓	✗ Opt-out	✓
Consumer Rights	✓	✓	✓	✓	✓
Employee and Business-to-Business (B2B) Contact Rights	✓	✗	✗	✗	✗
Data Governance Requirements	✓ Scope unclear; Regulations TBD	✓	✓	✗	✓
Vendor Contract Requirements	✓	✓	✓	✗	✓

First CCPA Enforcement Action

- Cal. AG brought first enforcement action, against Sephora, under CPPA for not offering opt-out from third-party tracking cookies and not recognizing Global Privacy Control signals
- Suggests that GPC is not optional for CCPA-covered businesses
- Judgment describes Sephora's contracts with third-party adtech vendors as "not valid service provider contracts" (emph. added)

What to Expect in 2023



Expanding Federal Regulatory Landscape

Regulatory Trends

- Cybersecurity Incident Disclosure Laws
- Comprehensive Cybersecurity Program
- Governance Practices
- False Claims Act Litigation

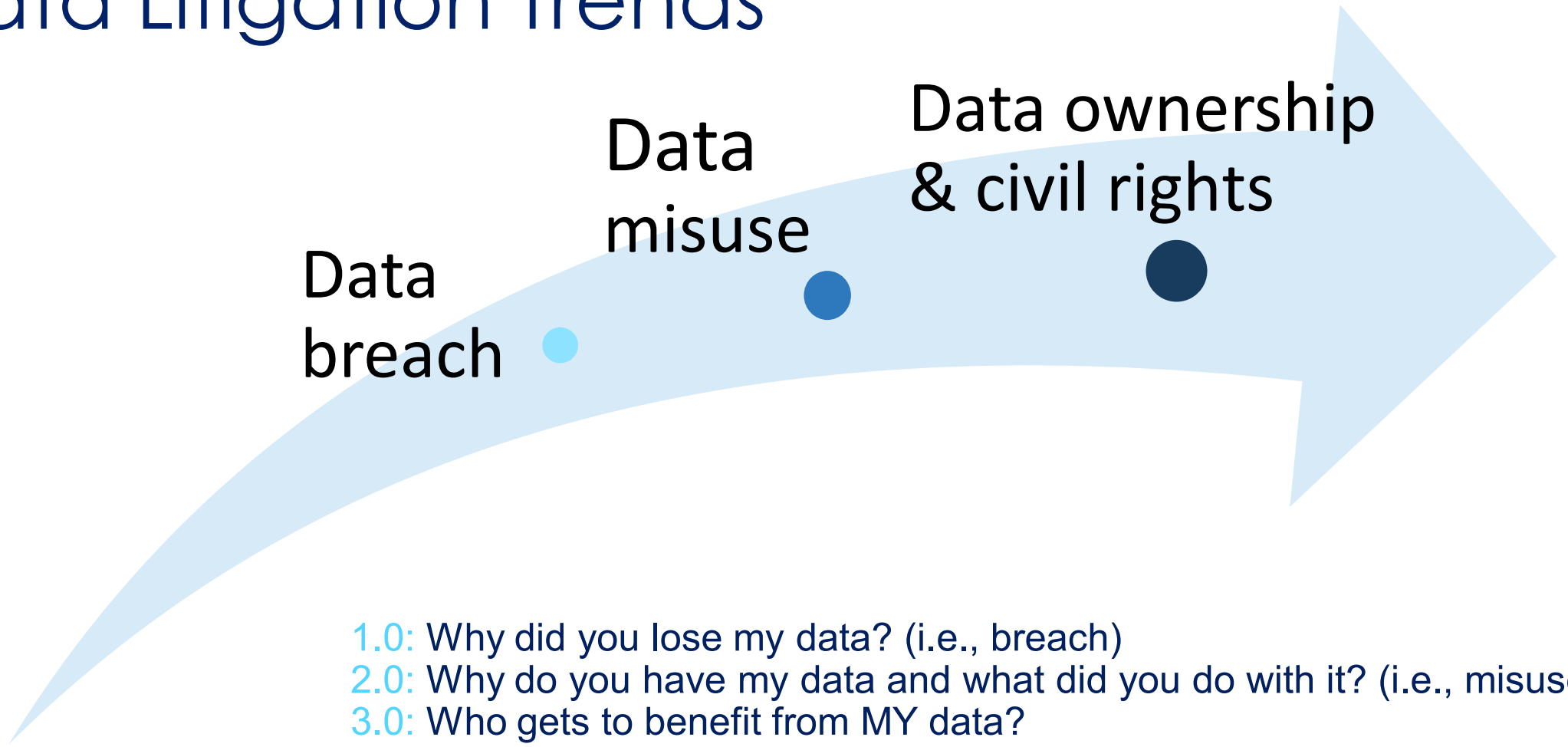
Sample Regulations in Past Year

- Cyber Incident Reporting for Critical Infrastructure Act
- OCC/FRB/FDIC: Banking organizations disclose cyber incidents
- FTC: Financial institutions develop cybersecurity risk management program
- SEC proposed cyber incident and governance disclosures for public companies
- DOJ Civil Cyber-Fraud Initiative

IP, Privacy and Business

- Legal
  - Ethical obligations
  - Confidentiality
  - Financial and other technology
- Types of data and industry
- Uses of data
  - Advertising
  - Customer facing information
  - Research, including search and sales trends
  - Derivative data
- IP
  - Copyright, trademark and patent
  - Mining
  - Technology

Data Litigation Trends



1.0: Why did you lose my data? (i.e., breach)
2.0: Why do you have my data and what did you do with it? (i.e., misuse)
3.0: Who gets to benefit from MY data?

Cases About Who Benefits from MY Data

As Technology, the Law and Society Change…….

What's Next?

- Ownership and valuation disputes
- Biometrics
- New applications of state anti-wiretapping statutes
- Video Privacy Protection Act
- Artificial intelligence and disparate impact claims
- Shareholder derivative/securities cases based on data-related disclosures

Website Wiretap Cases

Healthcare Providers

- *Partners Healthcare* (Mass. Sup. Ct.) – Settled $18.4 million
- *Sutter Health* (CA Sup. Ct.) - MTD 3rd Am. Compl. pending
- Dozen cases recently filed in N.D. Cal. against Meta for providers' use of Pixel

In re Facebook

- Mid-2020 9th Cir. revived claims that Facebook unlawfully intercepted logged-out users' browsing histories
- Settled March 2022 for $90MM

Session Replay

Mixed results, but largely favorable for defendants

Nike (C.D. Cal. 2021) – mouse movements, clicks, typing, IP address, etc. not "content"

Assurance (9th Cir. 2022) – Retroactive consent insufficient; has triggered new wave of cases in CA re session replay and chatbots

Google Search Cases

- Incognito (N.D. Cal., J. Koh) – wiretap claims alive
- App Analytics (N.D. Cal., J. Seeborg) – no interception; privacy settings not contract
- Chrome (N.D. Cal., J. Gonzalez-Rogers) – MSJ pending

Misc.

- *Smart speaker cases* (N.D. Cal. & Mass.) – largely dismissed on MTDs
- *Bose Headphones* (N.D. Ill.) – settled on individual basis after wiretap claims dismissed

Insurance Considerations

- Cyber insurance
- Malpractice insurance
- Business owner's liability insurance
- Other insurance considerations

Questions & Conversation

Holland & Knight

Connecticut Poised to Enact Consumer Privacy Law

Proposed Legislation Draws Heavily from Virginia, But Further Complicates Landscape

May 3, 2022

Holland & Knight Alert

Ashley L. Shively | Rachel Marmor

Highlights

- Connecticut has positioned itself to become the fifth state to implement comprehensive consumer privacy legislation, after both chambers of the state legislature approved draft bill SB 6 in late April.
- Connecticut's "Act Concerning Personal Data Privacy and Online Monitoring" adopts the same approach as the Virginia Consumer Data Protection Law (VCDPA), with only minor variations. The bill will become law if signed by Gov. Ned Lamont or if no action is taken by mid-May.
- This Holland & Knight alert provides key details on Connecticut's consumer privacy legislation and a comparison with four other states that have passed similar privacy legislation.

Connecticut has positioned itself to become the fifth state to implement comprehensive consumer privacy legislation, after both chambers of the state legislature approved draft bill SB 6 on April 22, 2022, and April 28, 2022, respectively. The "Act Concerning Personal Data Privacy and Online Monitoring" adopts the same approach as the Virginia Consumer Data Protection Law (VCDPA), with only minor variations. The bill will become law if signed by Gov. Ned Lamont or if no action is taken by mid-May.

The following tables compare the Connecticut bill to the laws of the four other states that have passed comprehensive consumer privacy legislations. A State Consumer Privacy Laws "cheat sheet" is also available for download.

Overview

With the passage of SB 6, some trends become clear: California is an outlier in extending rights to workforce members and business-to-business contacts. It is also an outlier in containing any sort of private right of action – the laws of the other four states can only be enforced by state regulators. The emerging trend is for laws to require notice and certain consumer rights, opt-in consent for processing of sensitive personal information in some circumstances, data minimization and other data management obligations, to require data protection impact assessments, and protection of personal information when shared with vendors.

Holland & Knight

Overview					
	California	Virginia	Colorado	Utah	Connecticut
Effective	California Privacy Rights Act (CPRA) fully effective Jan. 1, 2023	Jan. 1, 2023	July 1, 2023	Dec. 31, 2023	July 1, 2023
Private Right of Action	✓ Data breach only	✗	✗	✗	✗
Notice At/Before Collection	✓	✓	✓	✓	✓
Opt-In Default for Sensitive Personal Information (SPI)	✗ Opt-out	✓	✓	✗ Opt-out	✓
Consumer Rights	✓	✓	✓	✓	✓
Employee and Business-to-Business (B2B) Contact Rights	✓	✗	✗	✗	✗
Data Governance Requirements	✓ Scope unclear; Regulations TBD	✓	✓	✗	✓
Vendor Contract Requirements	✓	✓	✓	✗	✓

View larger image

Consumer Rights

The Connecticut bill, if it becomes law, will create new rights for Connecticut residents similar to those of consumers in Virginia and Colorado. The few minor distinctions in SB 6 include an explicit requirement to obtain consent to sell the personal information of a minor between ages 13-16 or process such information for advertising – an expansion past Virginia, which only requires opt-in consent up to age 13, to align with California.

Connecticut followed the approach of recent VCDPA amendments by including language related to the deletion right that allows for businesses to address issues of repopulating data feeds by opting the consumer out of processing, instead of full deletion. But since the other three states do not offer that option, it is unclear whether this will provide operational relief.

Holland & Knight

Consumer Rights					
	California	Virginia	Colorado	Utah	Connecticut
Know / Access	✓	✓	✓	✓	✓
Correction	✓	✓	✓	✗	✓
Deletion	✓ Limited to data obtained from the consumer	✓	✓	✓ Limited to data obtained from the consumer	✓
Restrict Sensitive Personal Information (SPI) Processing	✓	✓	✓	✓	✓
Opt-Out of Sales/Sharing/ Targeted Advertising	✓	✓	✓	✓	✓
Opt-In for Sales/Sharing/ Targeted Advertising for Minors	✓ To age 16	✓ To age 13	✓ To age 13	✓ To age 13	✓ To age 16
Opt-Out of Profiling/ Automated Decision-making		✓	✓	✗ Silent	✓
Non-Discrimination	✓	✓	✓	✓	✓

View larger image

Request Submission and Handling

On the submission and handling of consumer rights requests, Connecticut's new law closely parallels the Colorado Privacy Act (CPA) as opposed to Virginia. Connecticut follows California and Colorado in setting forth a requirement that businesses allow consumers to opt-out of targeted advertising or sale via an opt-out preference signal sent by some sort of technical mechanism (such as a user-enabled browser control). Unlike California and Colorado, however, there is no requirement in the Connecticut law that specifications for the technical mechanism be approved by the state regulator, creating uncertainty as to whether industry norms can develop around user-enabled controls.

Holland & Knight

Request Handling					
	California	Virginia	Colorado	Utah	Connecticut
Requests Must Be Verified	✓ Except opt-out/restrict SPI	✓	✓	✓	✓
Requires Separate "Opt-Out" Page	✓	✗	✓	✗	✓
Honor User-Enabled Browser Control	✓	✗	✓ By July 1, 2024	✗	✓ By Jan. 1, 2025
Accept Requests from Authorized Agents	✓	✗	✓ Opt-out only	✗	✓ Opt-out only
Timeline to Respond to Consumer Rights Requests	45 days, but 10 days for opt-out	45 days	45 days	45 days	45 days
Consumer Can Appeal Handling of Consumer Rights Request	✗	✓	✓	✗	✓

View larger image

Information Governance

All five of the laws being implemented in 2023 expand past the consumer-facing requirements put in place by California in 2020 through the California Consumer Privacy Act (CCPA) and require businesses to implement certain obligations related to the handling of data from all consumers.

Holland & Knight

Information Governance					
	California	Virginia	Colorado	Utah	Connecticut
Data Minimization	✓	✓	✓	✗	✓
Purpose and Use Limitations	✓	✓	✓	✗	✓
Disclose Retention Periods	✓	✗	✗	✗	✗
Data Privacy Impact Assessments	✓ Scope unclear; Regulations TBD	✓	✓	✗	✓
Reasonable Security	✓	✓	✓	✓	✓

View larger image

Enforcement

Connecticut follows the trend in allowing violations to be enforced only by its state Attorney General. Like Colorado, the Connecticut attorney general must provide a 60-day notice and opportunity to cure violations. The cure window, however, sunsets at the end of 2024. Violations of SB 6 are treated as a deceptive trade practice under the state Unfair and Deceptive Acts and Practices (UDAP) statute, and punishable by civil penalties of up to $5,000 plus actual and punitive damages and attorneys' fees and costs. California continues to be the only state to allow a private right of action – limited to certain types of data breaches only.

Holland & Knight

Civil Enforcement					
	California	Virginia	Colorado	Utah	Connecticut
Regulator	California Privacy Protection Agency	Attorney General	Attorney General and District Attorneys	Attorney General	Attorney General
Civil Penalties / Administrative Fines	$2,500 - $7,500	Up to $7,500, plus reasonable investigation and attorney expenses	Up to $20,000 per violation under Colorado Consumer Protection Act	Actual damages to the consumer and $7,500 per violation in civil penalties	Up to $5,000 under CT Unfair Trade Practice Act, plus actual and punitive damages, costs, and reasonable attorneys' fees
Cure Opportunity	✗ Regulatory cure period eliminated in California Privacy Rights Act (CPRA)	✓ 30-day cure period	✓ 60-day cure period through 2024	✓ 30-day cure period	✓ 60-day cure period through 2024; In 2025, cure opportunity at discretion of attorney general
Rulemaking Authority for Regulator	✓	✗	✓	✗	✗ Working group to study potential amendments
Regulator May Issue Guidance	✗ Eliminated in CPRA	✗	✓	✗	✗

View larger image

For more information or questions regarding Connecticut's consumer privacy legislation, its impact or relation to the four other state privacy laws, contact the authors or another member of Holland & Knight's Data Strategy, Security and Privacy Team.

Ashley L. Shively is a privacy attorney and class action litigator in Holland & Knight's San Francisco

office.

Ms. Shively counsels public and private companies on consumer protection and data privacy issues with respect to product development, sign-up and point-of-sale procedures, digital marketing, regulatory compliance, incident response, and state and federal enforcement. She regularly advises on the Children's Online Privacy Protection Act (COPPA), Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003, Fair Credit Reporting Act (FCRA), Gramm-Leach-Bliley Act (GLBA), state privacy and unfair and deceptive practices laws, and similar legal and regulatory requirements. At present, she is particularly focused on the comprehensive privacy laws enacted in California, including the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA), as well as analogous laws passed in Colorado (Colorado Privacy Act, or CPA) and Virginia (Consumer Data Protection Act, or CDPA) and similar legislation under consideration in other states.

415.743.6906 | Ashley.Shively@hklaw.com

Rachel Marmor is a privacy attorney in Holland & Knight's Boston office. Ms. Marmor counsels clients on a range of legal issues related to data strategy, consumer and employee privacy compliance, transaction risk and emerging technologies.

617.854.1436 | Rachel.Marmor@hklaw.com

Holland & Knight

SEC Proposes Cybersecurity Incident and Governance Disclosure Obligations for Public Companies

March 14, 2022

Holland & Knight Alert

Scott Mascianica | Shardul Desai | Ira N. Rosner

Highlights

- Less than a month after the U.S. Securities and Exchange Commission (SEC) proposed substantial new cybersecurity requirements for investment advisers and registered investment companies, the commission unveiled a new slate of proposed cybersecurity disclosure rules for public companies.
- If adopted, the proposed rules would require each public company to report material cybersecurity incidents within four business days after determining that it has experienced such incidents, provide periodic updates of previously reported cybersecurity incidents, describe its cybersecurity risk management policies and procedures, disclose its cybersecurity governance practices and disclose cybersecurity expertise on the board of directors.
- The proposed rules seek to have public companies disclose cybersecurity incidents and their risk management, strategy and governance practices in a consistent and comparable manner.

Less than a month after the U.S. Securities and Exchange Commission (SEC) proposed substantial new cybersecurity requirements for investment advisers and registered investment companies, the commission unveiled a new slate of proposed cybersecurity disclosure rules for public companies. The proposed rules, if adopted, would require each public company to: 1) report material cybersecurity incidents within four business days after determining that it has experienced such incidents; 2) provide periodic updates of previously reported cybersecurity incidents; 3) describe its cybersecurity risk management policies and procedures; 4) disclose its cybersecurity governance practices; and 5) disclose cybersecurity expertise on the board of directors.[1]

SEC Chair Gary Gensler previewed the possibility of such proposed rules during his January 2022 speech at the Northwestern Pritzker School of Law's Annual Securities Regulation Institute. The proposed rules seek to have public companies disclose cybersecurity incidents and their risk management, strategy and governance practices in a consistent and comparable manner. The proposed rules, however, may create significant litigation and enforcement risks for public companies and could potentially expose them to greater cybersecurity risks in certain situations. Furthermore, the contemplated ongoing reporting obligations and proposal that companies consider incidents at third-party providers as part of their assessment would place significant burdens on public companies. Additionally, the proposed rules are the latest example of the SEC using its rulemaking and enforcement authority to dictate corporate governance and board composition at public companies.

This Holland & Knight alert provides a summary of the new proposed rules and offers some key takeaways.

Proposed Cybersecurity Requirements for Public Companies

A. Current Reporting about Material Cybersecurity Incidents

The SEC proposed to amend Form 8-K to require public companies to disclose, within four business days after the company determines that it has experienced a material "cybersecurity incident," certain information about the incident. Under the proposed Item 1.05 to Form 8-K, a "cyber incident" is defined as "an unauthorized occurrence on or

conducted through a registrant's information systems that jeopardizes the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein." The SEC stated that "cybersecurity incident" should be "should be construed broadly…" and may include an accidental exposure of data.

Although the SEC does not expect a public company to disclose technical information about its cybersecurity systems, potential vulnerabilities or response to a cybersecurity incident, disclosure of the following information for each material cybersecurity incident would be required:

- when the incident was discovered and whether it is ongoing
- a brief description of the nature and scope of the incident
- whether any data was stolen, altered, accessed or used for any other unauthorized purpose
- the effect of the incident on the company's operations
- whether the company has remediated or is currently remediating the incident[2]

Notably, the triggering event for disclosure is *not* the date of the cybersecurity incident. Rather, disclosure would be within four days after the company "determines that a cybersecurity incident it has experienced is material."[3] Notwithstanding allowing the exercise of discretion (which effectively codifies the longstanding concept of "ripeness" in determining materiality), the SEC expects public companies "to be diligent in making a materiality determination."[4]

Materiality is to be determined under longstanding precedent of whether there is a substantial likelihood that a reasonable shareholder would consider the information as important or as having significantly altered the total mix of information made available.[5] The SEC acknowledged that this materiality analysis "is not a mechanical exercise" but rather would require the company to "thoroughly and objectively evaluate the total mix of information…"[6]

The SEC proposes to make the cybersecurity incident reporting on Form 8-K eligible for a limited safe harbor from liability under Section 10(b) or Rule 10b-5 under the Exchange Act for failure to timely file.[7] Importantly, however, this limited safe harbor does not exempt companies from antifraud liability – or other liability under other provisions of the federal securities laws – for representations made in a Form 8-K concerning the cybersecurity incident.[8]

B. Cybersecurity Incident Disclosure in Periodic Reports

The SEC proposed to add new Item 106 to Regulation S-K and updates to Forms 10-Q and 10-K that will require public companies to provide periodic updates about previously disclosed cybersecurity incidents when a material change, addition or update has occurred. The SEC justifies the ongoing reporting requirement to "balance the need for prompt and timely disclosure regarding material cybersecurity incidents with the fact that a registrant may not have complete information about a material cybersecurity incident at the time it determines the incident to be material."[9] The SEC's proposed rule does not require that public companies file a separate Form 8-K for such updates; rather, this information would be disclosed in the next filed quarterly or annual report.[10]

Similarly, if a public company discovered that a series of previously undisclosed, immaterial cybersecurity incidents had become material in the aggregate, the company will need to disclose such incidents in its next filed periodic report. Information to be provided under the SEC's proposed Item 106(d)(2) would be similar to the proposed Form 8-K Item 1.05 information detailed above.

In both instances, the SEC provided a list of information public companies *should* include under proposed Instructions to Item 106(c), such as the material impact on the company's operations and whether the company has remediated the incident.

C. Periodic Disclosures of Cybersecurity Risk Management Policies and Procedures

The SEC also proposed Item 106(b) of Regulation S-K, which would require significant disclosure about a public company's policies and procedures to identify and manage cybersecurity risks. Specifically, the proposed rule would require public companies to disclose "in such detail as necessary to adequately describe the registrant's policies and procedures, if it has any, for the identification and management of risks from cybersecurity threats … " Items "that would require disclosure" would include[11]:

- if the company has a cybersecurity risk assessment program and, if so, a description of the program
- whether the company engages consultants and other third parties in connection with any cybersecurity risk assessment program
- the company's policies and procedures to oversee and identify the cybersecurity risks associated with the use of any third-party service provider, including whether and how cybersecurity considerations impact selection and oversight of these providers
- activities the company undertakes to prevent, detect and minimize effects of cybersecurity incidents
- whether the company has business continuity, contingency and recovery plans in the event of a cybersecurity incident
- previous cybersecurity incidents that have informed changes in the company's cybersecurity governance, policies and procedures, and technologies
- cybersecurity risks and incidents that have affected or are reasonably likely to affect the company's results of operations or financial condition and, if so, how
- how cybersecurity risks are considered as part of the company's business strategy, financial planning and capital allocation

D. Governance Disclosures Regarding Cybersecurity

The SEC also proposed two additional items under Regulation S-K, which would require public companies to make three governance-related disclosures concerning: 1) board oversight of cybersecurity risks and associated processes; 2) management's role in assessing and managing cybersecurity risks and implementing the company's cybersecurity policies and procedures; and 3) cybersecurity expertise of members of the board, if any.

With respect to the board's oversight of cybersecurity risks, disclosure under the proposed Item 106(c)(1) of Regulation S-K includes the following nonexclusive items:

- whether the entire board, specific board members or a board committee is responsible for the oversight of cybersecurity risks
- the process by which the board is informed about cybersecurity risks
- the frequency with which the board is informed about cybersecurity risks
- whether and how the board or board committee considers cybersecurity risks as part of its business strategy, risk management and financial oversight

With respect to management's role in assessing and managing cybersecurity risks and implementing a company's cybersecurity policies and procedures, disclosure under proposed Item 106(c)(2) of Regulation S-K "should include" the following nonexclusive items:

- whether certain management positions or committees are responsible for managing and measuring cybersecurity risks
- whether the company has a designated chief information officer, security officer or someone in a comparable

position

- the processes by which such person or committee is informed about and monitors prevention, mitigation, detection and remediation of cybersecurity incidents
- whether and how frequently such person or committee reports to the board of directors or a committee of the board on cybersecurity risks

Finally, the SEC proposes revisions to Item 407 of Regulation S-K to require public companies to: 1) disclose the cybersecurity expertise of its board members, if any; 2) name the directors; and 3) detail their experience. Although the SEC declined to define "cybersecurity expertise," it offered an illustrative, nonexclusive list of factors to help assess such expertise.

Importantly, the SEC clarified that any person identified to have cybersecurity expertise is not an expert for any purposes of Section 11 of the Securities Act and does not impose any additional duties, obligations or liability on this individual.

Key Takeaways

- **These Rules Create Significant Litigation and Strategic Risks:** The cybersecurity incident disclosure obligation would require that public companies disclose specific details concerning the cybersecurity incident, scope of the incident, data accessed or stolen, and effect of the incident on company operations. By requiring this disclosure four days after determination of a material cybersecurity incident, the Form 8-K filing could precede data breach notices to state attorneys general, individuals and potentially impacted business partners. Further, providing such details prior to the completion of a forensic investigation and data-mining efforts is likely to expose companies to litigation before it has a full picture of the impact of the cybersecurity incident, as well as potentially undermine attorney-client and work product privilege associated with investigating the cybersecurity incident.

  Additionally, both the cybersecurity incident disclosures (including its associated periodic reporting) and disclosure of the company's cybersecurity risk management policies and procedures would create significant risks that the SEC's Division of Enforcement and private litigants will seize on the company's representations as potential bases for liability under the antifraud provisions and otherwise after an incident. As demonstrated in the First American Financial Corporation action last year, the SEC's Division of Enforcement has already shown a willingness to utilize controls and procedures provisions of federal securities laws to hold companies liable in connection with cybersecurity incidents. The additional line item disclosure requirements of proposed Items 106 and 407 of Regulation S-K undoubtedly will present risks that the Division of Enforcement will utilize such provisions to penalize companies after they have been the victims of a cybersecurity incident. This is particularly the case in the short term, where interpretative guidance may be limited and SEC policy regarding enforcement of the new rules may not be fully understood.

- **These Rules May Create Significant Cybersecurity Risks:** Although the SEC claims that these disclosure rules do not seek technical information, the proposed rules would require disclosure of substantial details concerning cybersecurity incidents and public companies' cybersecurity risk management policies and procedures. Although the SEC appears to believe that disclosures regarding public companies' cybersecurity programs could lead to improvement of their policies and procedures, such detailed disclosure could have the unintended result of making them more vulnerable to cyberattacks. For example, the public disclosure of detailed information concerning a cybersecurity incident prior to full containment and remediation could provide opportunities for cybercriminals to further target victim companies and their affected customers, employees or other constituents. Additionally, cybercriminals could potentially utilize a company's disclosures concerning its cybersecurity policies and

procedures, such as the activities that a public company takes to detect cybersecurity incidents, to identify vulnerabilities and to design strategic cyberattacks against the company.

Additionally, in many instances, this will force public companies to engage in ongoing disclosure about incidents while in the midst of incident response and remediation. The unintended consequences of such disclosures on these efforts could be significant. For example, in the case of a ransomware attack, such disclosures could impact a company's ransomware negotiation position and strategy.

- **Once Again, Risks and Incidents at Third Parties Could Create Disclosure Obligations**: The SEC highlighted companies' "increasing reliance on third party service providers for information technology services…" as one of the reasons cybersecurity risks have increased.[12] As with the proposed rule for investment advisers and companies, the SEC's proposed definition of information systems includes "information resources owned or used by the registrant…[13] In the event of a cybersecurity incident at a third-party vendor, public companies may have difficulty obtaining timely information to make a materiality determination for information systems they do not own or to provide sufficient details that would be required under the proposed rules.

  As a result, public companies (and companies considering becoming publicly traded) may need to reassess their cybersecurity and data privacy risks associated with their vendor management programs. This may include conducting due diligence reviews, conducting cybersecurity audits, including contractual provisions to ensure timely and detailed cyber incident reporting, or reconsidering the mix of internal and outsourced information technology systems.

- **Additional Burden of Ongoing Reporting**: Public companies would be subject to ongoing reporting obligations if the SEC adopts the proposed rules. The ongoing reporting requirements for prior cybersecurity disclosures will force public companies to spend significant time and resources implementing protocols that allow for analysis and assessment of *ongoing and prior* cyber incidents. Given that a materiality assessment is fluid, this would require public companies to engage in frequent assessments of prior cyber incidents, including those previously deemed not material, to assess possible disclosure obligations.

  Furthermore, the ongoing reporting requirement would create an ancillary obligation for public companies to repeatedly assess their prior incident disclosures. Although companies could potentially use the ongoing update requirement as a mechanism for correcting prior disclosures, the SEC indicated that prior Forms 8-K concerning cybersecurity disclosures could be deemed false or misleading unless corrected.

- **No Delay Reporting Safe Harbor**: Most state laws permit companies to delay data breach notices when law enforcement determines that such notices will impede an investigation. The SEC's proposed rules include no such exception, instead stating that "[o]n balance, it is our current view that the importance of timely disclosure of cybersecurity incidents for investors would justify not providing for a reporting delay."[14] The SEC acknowledged that the lack of delay notice can create inconsistent disclosure requirements for public companies at the state and federal level.[15] Although many public companies already deal with such legal differences between state and federal disclosure laws, the lack of a safe harbor that primarily aims to aid law enforcement in identifying and prosecuting the criminal actors appears at odds with the government's broader cybersecurity goals.

- **Difficulties Fulfilling Board Seats with Cybersecurity Expertise:** Currently, there is a substantial talent shortage of cybersecurity professionals. As a result, individuals who would be qualified to become board members and have cybersecurity expertise are likely short in supply. Nevertheless, by requiring the disclosure of cybersecurity expertise of board members, many companies may attempt to fill a board seat with someone with such cybersecurity

expertise. Smaller public companies may find it difficult to attract sufficiently qualified individuals and find themselves at a comparative disadvantage to larger companies that could provide better incentives to those individuals. The need to find board members with cyber expertise also may compete with other board composition requirements faced by public companies.

- **Governance Insight:** While not an express purpose of the proposed rules, there is little doubt that they reflect the SEC's desire to influence corporate governance at public companies. As SEC Commissioner Hester M. Pierce identified in her dissenting statement, the proposed rules will likely affect the composition of boards of directors and management teams and result in substantive changes to management cybersecurity policies and procedures.[16] The proposed rules will also likely influence public companies to adapt their cyber risk management policies so that they will be viewed favorably in light of the specific disclosure requirements. This is not the first time that the Congress or the SEC has used disclosure obligations to dictate substantive changes in corporate management.[17] As noted above, however, the proposed rules are likely to have pervasive and unintended effects, such as creating tension between disclosure of cyberattacks and preserving law enforcement's ability to investigate and pursue wrongdoing. Regardless, the proposed rules will require public companies to devote increased time and financial resources to cyber risk management, governance and oversight – if nothing else, "to avoid appearing as if they do not take cybersecurity as seriously as other companies."[18]

The SEC's proposed rules are open for comment until 30 days after publication in the federal registrar or May 9, 2022 (whichever is later). The SEC will then assess public comments and vote on a final rule.

For more information about the cybersecurity requirements for public companies and other registrants, contact the authors. In addition, as the SEC continues to develop cybersecurity requirements for regulated entities, you can receive updates by following Holland & Knight's SECond Opinions and Cybersecurity and Privacy blogs.

Notes

[1] For purposes of this alert, all references are to the U.S. issuer rules. However, the SEC's rule proposal also applies to foreign private issuers and includes parallel rule proposals for those entities. For example, the proposed Form 8-K rule would also apply to foreign private issuers based on similar proposals in connection with Form 6-K.

[2] As contemplated by the rule, public companies will need to assess potential cybersecurity incidents not only on the systems that they own, but also on information resources "used by" the company, including cloud-based storage devices and virtual infrastructure.

[3] Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure Proposed Rule ("Proposed Rule"), at 22. Please see our prior analysis on the proposed cybersecurity rules for investment advisers and investment companies for details on the significant differences in incident reporting timelines.

[4] Proposed Instruction 1 to Item 1.05 states that "a registrant shall make a materiality determination regarding a cybersecurity incident as soon as reasonably practicable after discovery of the incident." Proposed Rule, at 22; Proposed Instruction 1 to Proposed Item 1.05 of Form 8-K.

[5] See, e.g., *Basic, Inc. v. Levinson*, 485 U.S. 224, 232 (1988); *TSC Industries v. Northway, Inc.,* 426 U.S. 438, 449 (1976).

[6] Proposed Rule, at 23.

[7] *Id.* at 27; Proposed Exchange Act Rules 13a-11(c) and 15d-11(c).

[8] Notably, a failure to timely file an Item 1.05 Form 8-K would not affect a public company's ability to register securities

on Form S-3.

[9] *Id.* at 32.

[10] However, the SEC did note that a public company may need to file an amended Form 8-K to correct a prior disclosure that becomes inaccurate or materially misleading in light of subsequent developments. *Id.* at 33, FN 69.

[11] It is unclear if the actual proposed rule includes a mandated list of disclosure items. Unlike the body of the proposed rule release, which notes that proposed Item 106(b) "would require disclosure," the proposed rule itself notes that a discussion "should include." We expect that the comments and responses thereto will bring greater clarity on whether the list outlined above is illustrative or mandatory.

[12] *Id.,* at 7; see also *Id.* at FN 10.

[13] Proposed Item 106(a)(3).

[14] *Id.* at 25.

[15] "To the extent that proposed Item 1.05 of Form 8-K would require disclosure in a situation in which a state law delay provision would excuse notification, there is a possibility a registrant would be required to disclose the incident on Form 8-K even though it could delay incident reporting under a particular state law." *Id.* at 26.

[16] See Dissenting Statement on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure Proposal of Commissioner Hester M. Pierce.

[17] Other examples include relatively low reporting thresholds for environmental proceedings to encourage environmental law compliance, Compensation Disclosure and Analysis to influence compensation decisions, changes to audit committees and the auditor relationship caused by Sarbanes-Oxley required disclosures and changes to compensation committee activities caused by Dodd-Frank.

[18] See FN 16.

Holland & Knight

Scott F. Mascianica is an experienced investigative and litigation attorney and a member of Holland & Knight's White Collar Defense and Investigations Team and the Securities Enforcement Defense Team. With more than 15 years of experience in the government and private sectors, Mr. Mascianica focuses his national practice on conducting internal investigations for public-company issuers and other financial institutions, representing individuals and entities in investigations by the U.S. Securities and Exchange Commission (SEC) and U.S. Department of Justice (DOJ), as well as advising issuers, financial services firms and regulated entities on regulatory and compliance matters.

214.969.2106 | Scott.Mascianica@hklaw.com

Shardul Desai is a cybersecurity, data privacy, and white collar defense and government investigations attorney in Holland & Knight's Washington, D.C. office. Mr. Desai has extensive experience in handling cyber intrusions and data breaches, trade secret thefts, emerging technology matters and complex white collar investigations. With a computer science and physics background, Mr. Desai is highly skilled and knowledgeable to advise companies on novel issues at the intersection of law, technology and data privacy.

202.469.5210 | Shardul.Desai@hklaw.com

Ira N. Rosner is an attorney in Holland & Knight's Miami office. He has nearly four decades of experience helping entrepreneurs and corporate management teams create, fund, manage, grow and capitalize on their businesses. Mr. Rosner has worked with a wide variety of companies, ranging from startup ventures to Fortune 100 enterprises, in a wide array of industries, including financial technology (FinTech) and financial services, construction, real estate (including REITs), healthcare, pharmaceuticals, aerospace and aviation, agriculture, energy, manufacturing, high tech, life sciences, retail, business outsourcing, telecommunications and insurance.

305.789.7556 | Ira.Rosner@hklaw.com

Holland & Knight

Manipulative Online Design Tactics Become Riskier

September 21, 2022
Holland & Knight Alert
Wendell Bartnick

Highlights

- The Federal Trade Commission (FTC) has issued guidance on the use of dark patterns, warning companies that it will increasingly focus its enforcement efforts on deceptive and manipulative tactics on websites and mobile applications.
- A "dark pattern" is a user interface design method on a website or mobile application that results in a substantial number of users making choices that they otherwise would not make that benefit the provider of the website or application rather than the users.
- Companies that use dark patterns on websites and mobile applications to deceive or manipulate consumers into taking detrimental actions may receive scrutiny from the FTC. Companies should take the necessary steps to review their websites and mobile applications to mitigate this risk.

In recent years, the use of clickbait and dark patterns has attracted the attention and scorn of state legislatures, the Federal Trade Commission (FTC), state attorneys general, consumer advocates and consumers. Three state privacy laws attempt to specifically address the use of dark patterns to obtain consent in a privacy context. The FTC has issued a request for public comment to update its current ".com Disclosures" guidance, issued an enforcement policy statement warning companies that it will increasingly focus its enforcement efforts on deceptive sign-up and cancellation tactics involving negative option marketing and operation, has investigated companies for difficult cancellation processes and, most recently, published its "Bringing Dark Patterns to Light" staff report (the Report). State attorneys general and consumer advocate organizations have submitted comments, including this example, to the FTC asserting their displeasure with clickbait and dark patterns.

This Holland & Knight alert will focus on dark patterns and the FTC's Report published in September 2022.

Example Dark Patterns Highlighted by the FTC

A "dark pattern" is commonly defined as a user interface design method on a website or mobile application that results in a substantial number of users making choices that they otherwise would not make that benefit the provider of the website or application rather than the users. The FTC calls them manipulative design tricks and psychological tactics and stated that dark patterns are "found in a variety of industries and contexts, including ecommerce, cookie consent banners, children's apps, subscription sales, and more."

Examples of design methods that the FTC may deem to be dark patterns:

- use company-preferred pre-checked boxes, default settings and prominent options
- give illusory choices
- use confusing toggle settings
- bury key limitations of a product or service in dense terms of service documents
- require scrolling to see material terms
- use nondescript or small icons tooltips,

- bury settings and use vague setting names
- implement long/difficult subscription cancellation process
- display countdown timers on offers that are not truly time-limited
- falsely claim that a product is almost sold out
- falsely claim that others are looking at, or recently bought, the same products
- use double negatives
- deceptively format advertisements to appear as independent, editorial content
- deceptively format as a neutral comparison-shopping site, but rank by compensation
- falsely suggest affiliation with reputable organizations
- hyperlinks, pop-ups or drop-down menus that require a hover or click to view material terms
- display material terms in normal unbolded text in the middle of bolded text that does not contain material terms
- deceptively offer free trials, hiding cancellation terms
- display hard-to-find or hard-to-read disclosures
- delay disclosure of fees until late in the application/purchase process (e.g., drip pricing)
- use poor color contrast
- disguise purchases as part of game play
- repeatedly prompt users to re-make choices already made

FTC's Recommendations

Companies that use website and mobile application design practices to deceive or manipulate consumers into taking detrimental actions may receive scrutiny from the FTC. In the Report, the FTC made specific recommendations to help companies avoid using design methods in a manner that could be considered dark patterns that violate the FTC Act and other federal laws.

The Report indicates that companies should take at least the following steps to mitigate risk:

- consider design elements as a whole, because multiple dark patterns can have an even stronger effect, according to the FTC
- as part of A/B testing, consider whether higher conversion using one interface is due to manipulative design elements
- publish websites and mobile apps that do not create false beliefs or otherwise deceive and consider how an interface can increase consumer understanding of material terms
- consider the net impression of a website or mobile app, because disclaimers may not overcome deceptive design
- include accurate information about mandatory fees in the "upfront, advertised price"
- consider whether pricing practices treat consumers differently based on race, national origin or other protected characteristics
- when an interface targets a specific audience (e.g., children), consider how design choices will be viewed by that audience
- review subscription cancellation mechanisms and potentially reduce the complexity and number of screens of the cancellation process
- if telephone cancellation is permitted, review policies and procedures that apply to answering calls during normal

business hours and within a short time frame

- when accepting purchases online, consider the steps taken to ensure the accountholder is consenting to a purchase
- reevaluate the collection of personal information to minimize unnecessary collection
- consider taking steps to avoid subverting consumers' privacy choices by reviewing default settings, the steps consumers must take to make choices, the clarity and prominence of toggle options, and the use of just-in-time notices and choices related to the collection and use of sensitive personal information
- be transparent and accurate when collecting lead information and monitor third-party lead generators

Takeaways

The Report increases the risk to companies that use dark patterns, because the FTC will hold them accountable for not following its guidance. The Report's release coincides with current FTC enforcement activity, increased public discussion about dark patterns, and the FTC's conclusion that manipulative design techniques online are potentially more harmful than in the physical environment because more data can be collected about individuals to generate manipulative design elements and trying new techniques online is cheap and easy.

Moreover, the FTC will not limit its enforcement activity to negative option/subscription contracts where it has historically focused its attention. For example, large sections of the Report focus on the use of dark patterns to impact privacy-related consent and settings. The FTC's focus on privacy aligns with the privacy laws in California, Colorado and Connecticut that expressly state that consent requirements are not met if agreement is obtained through the use of dark patterns. The Utah and Virginia privacy laws also make clear that valid consent must be freely or voluntarily given in an informed manner. Regulators in Utah and Virginia may take the position that the use of dark patterns to obtain agreement is not informed and freely or voluntarily consent.

In addition to the federal and state regulatory compliance risk, companies that use dark patterns in the process of obtaining any legal agreement with consumers could risk future claims that an agreement was not formed or is voidable because there was no acceptance or meeting of the minds with respect to that agreement.

Companies should consider reviewing the user interface design of their websites and mobile applications to determine whether any of the techniques described in the Report are used to obtain consent or agreement from users. If so, the company can evaluate whether the use of the techniques are dark patterns and take steps to update them.

For more information on the FTC Report or companies needing assistance with review of user interface design methods to comply with the Report or other FTC guidance, contact the author or another member of Holland & Knight's Data Strategy, Security & Privacy Team or Consumer Protection Defense and Compliance Team.

Wendell J. Bartnick is a tech and data attorney in Holland & Knight's Houston office, where he counsels clients across various industries on privacy compliance, data protection and breaches, technology product development and commercialization, and e-commerce matters.

713.244.8216 | Wendell.Bartnick@hklaw.com

Holland & Knight

FTC Set to Update Endorsement Guides on Social Media Advertising

A Closer Look at the Proposed Changes and Their Impact on Your Business
June 15, 2022
Holland & Knight Alert
Anthony E. DiResta | Da'Morus A. Cohen | Benjamin A. Genn

Highlights

- The Federal Trade Commission (FTC) is poised to issue updated Endorsement Guides after a comment period on the proposed changes. The Guides still require advertisers to clearly and conspicuously disclose material connections between a brand and its endorsers, but the updates reflect societal and technological changes to advertising, including tightening of guidelines relating to posting fake positive reviews or suppressing negative reviews.
- The updates reveal the FTC's deepening enforcement priority in regulating social media.
- The proposed revisions add a new section highlighting advertising directed at children and discussing the capacity of children to differentiate advertising content, including through disclosures recognizable and understandable to them.

The Federal Trade Commission (FTC) is poised to issue updated Guides Concerning the Use of Endorsements and Testimonials in Advertising (the Guides) following a comment period on the proposed changes. This Holland & Knight alert provides an overview of the FTC's proposed updates and the potential impact on companies advertising through social media and similar channels.

Introduction: Social Media Advertising Is Regulated

Through the FTC Guides

Through publication of the Guides, the FTC seeks to advise businesses on the proper disclosures and methodology of endorsement and testimonial advertising, as enforced through Section 5 of the FTC Act. The Guides are advisory only – they are guidelines – but the FTC publishes them to put those in the marketplace on notice of what is expected to avoid an enforcement action under the FTC Act's deception sections.

Generally, the Guides define endorsements and testimonials as an advertising message that leads consumers to believe it depicts the opinions, beliefs or experience of someone other than the advertising business. These types of advertisements, as other advertisements, must be honest, truthful and non-misleading, and must reflect the actual opinions or experience of the endorser. This is especially true because the advertiser must be able to substantiate any claims of its endorsers, and endorser claims will be interpreted as representing a typical experience that consumers can also expect to have. (If this is not the case, a brand must clearly and conspicuously disclose what a typical experience would be.)

Moreover, the Guides require an "expert endorser" – one with the experience, training or knowledge superior to regular consumers – to have the qualifications so represented and that would give the expert endorser expertise in the area of endorsement.

Importantly, the Guides require an endorser to fully disclose any material connection between themselves and the brand, if that connection might materially affect the weight or the credibility of the endorsement. The endorser must

actually use the product when giving the endorsement (and "actual consumers" must be actual consumers, or otherwise clearly and conspicuously disclosed as not actual consumers), and brands may be liable for false or unsubstantiated endorser statements or for failing to disclose any material connection. Unsurprisingly, the endorser may also be liable for statements that he or she makes.

Brands should be aware that the FTC expects its decision-making process on endorsements to be formed by the collective judgment of the business, not by a siloed department or personnel.

Through FTC Enforcement Actions

The FTC has engaged in a number of enforcement actions involving social media, including a recent settlement against Fashion Nova. There, the FTC alleged that the fashion retailer misrepresented product reviews on its website – specifically, that the posted reviews represented the ratings of all customers who submitted a review, when the posted reviews really only represented the portion of reviews submitted with 4 stars or higher out of 5 stars. All other reviews posted to the website were suppressed. Through the settlement, the retailer is prohibited from suppressing customer reviews and agreed to pay the FTC $4.2 million.

Social media is also subject to review by state attorneys general through their "deception" jurisdiction.

Impact of Updated and Revised Guides

The FTC seeks comments on the revisions to the Guides online or in paper form and will publish the comments on Regulations.gov.

The proposed revisions to the Guides impact all businesses who engage in any form of social media advertising. The FTC continues to catch up to technological and societal advancements, especially in the advertising realm, and is not shy in bringing enforcement actions against bad actors in this space. In these actions, the FTC uses the same rules and regulations it has used for decades to enforce unfair and deceptive practices, this time expanding the scope to social media endorsers and the brands they advertise for.

As Commissioner Rebecca Kelly Slaughter stated last month, the FTC is attempting to bring more clarity, guidance and deterrence to this space. The goal of the Guides is to provide honest businesses with clear guardrails and not ambiguous hypotheticals.

The burden falls on all businesses to be aware of these developments and to comply with the rules and regulations enforced by the FTC. Thus, it is critical that all companies engaging in any form of social media advertising comply with the guardrails set forth in the Guides.

Businesses should especially be aware that:

- The proposed revisions represent the FTC's focus and interest on the deceptive practices of endorsers and their brands.
- Targeting specific audiences, including the elderly and children, requires audience-specific disclosures.
- Material connections must be clearly and conspicuously disclosed. Brands should determine whether they have "material" connections, then disclose them.
- Online reviews must be honest, real and not gated (i.e., a brand must not suppress negative reviews).

Proposed Revisions, Explained

Among the various proposed revisions to the Guides, there are many that brands should be aware of and comply with, as stated in the FTC's notice of proposed changes.

a. **Definition of "endorsement":** The proposed revisions would clarify the definition of "endorsement" to clarify that

"marketing" and "promotional" messages may be endorsements. The revised definition would also indicate that tags in social media posts can be endorsements.

b. **Fabricated endorsers:** Because an endorser could be an individual, group or institution, the revised Guides would apply to endorsements by fabricated endorsers.

c. **Bots, fake accounts:** It remains illegal to sell, purchase or use bots or other fake social media accounts to market goods and services.

d. **Purchasing or creating indicators:** It is a deceptive practice for users of social media to purchase or create indicators of social media influence.

e. **Definition of "product":** The Commission proposes modifying the definition to clarify that a "product" includes a "brand."

f. **Definition of "clear and conspicuous":** The proposed revisions add a new definition of "clear and conspicuous," meaning a disclosure that "is difficult to miss (i.e., easily noticeable) and easily understandable by ordinary consumers." The definition:

– gives specific guidance to visual and audible disclosures

– stresses the importance of "unavoidability" when the communication involves social media or the internet

– states that the disclosure should not be contradicted or mitigated by, or inconsistent with, anything in the communication

Generally, the format of the disclosure should be consistent with the format of the representation (i.e., when the triggering claim is visual, the disclosure should be at least visual).

g. **Targeting of an audience:** The definition of "clear and conspicuous" notes that when an endorsement targets a specific audience, such as older adults, its effectiveness will be evaluated from the perspective of members of that group.

– **New Section 255.6:** The Commission proposes adding a section stating: "Endorsements in advertisements addressed to children may be of special concern because of the character of the audience. Practices which would not ordinarily be questioned in advertisements addressed to adults might be questioned in such cases."

h. **Endorser liability:** Endorsers themselves may be subject to liability for their statements, including when they make representations that they know or should know to be deceptive. The level of due diligence required by the endorsers will depend on their level of expertise and knowledge, among other factors.

i. **Liability for intermediaries:** Intermediaries, such as advertising agencies and public relations firms, may be liable for their roles in disseminating what they knew or should have known were deceptive endorsements. In an example from the proposed revisions, advertising agencies may be liable when they intentionally engage in deception or that ignore obvious shortcomings of claims; they may also be liable if they fail to disclose unexpected material connections (by disseminating advertisements without necessary disclosures of material connection or by hiring and directing the endorsers who fail to make necessary disclosures).

j. **Images and likeness of people:** The use of an endorsement with the image or likeness of a person other than the actual endorser is deceptive if it misrepresents a material attribute of the endorser.

k. **Modification of past posts:** An endorser does not need to go back and modify or delete past social media posts as long as the posts were not misleading when they were made and the dates of the posts are clear and conspicuous to viewers. However, if the endorser or publisher reposts the post, it would suggest to reasonable consumers that the endorser continued to hold the views expressed in the prior post.

l. **Liability for paid endorser:** A paid endorser and the company paying the endorser are both potentially liable for the endorser's social media post that fails to disclose the endorser's relationship to the company.

m. **Seller agreements to display reviews:** In procuring, suppressing, boosting, organizing or editing consumer reviews of their products, advertisers should not take actions that have the effect of distorting or otherwise misrepresenting what consumers think of their products. This is true regardless of whether the reviews are considered "endorsements" under the Guides.

n. **When sellers are not required to display reviews:** Sellers are not required to display customer reviews that contain unlawful, harassing, abusive, obscene, vulgar or sexually explicit content, or content that is inappropriate with respect to race, gender, sexuality or ethnicity, or reviews that the seller reasonably believes are fake, so long as the criteria for withholding reviews are applied uniformly to all reviews submitted. Sellers are not required to display reviews that are unrelated to their products or services (such "services" include customer service, delivery, returns and exchanges).

o. **Paying for positive reviews:** Such reviews are deceptive, regardless of any disclosure of the payment, because the manufacturer has required that the reviews be positive.

p. **Solicitation of feedback from customers:** "Review gating" means practices that involve obtaining customer feedback and then sending satisfied and dissatisfied customers down different paths in order to encourage positive reviews and avoid negative reviews. Such disparate treatment may be an unfair or deceptive practice if it results in the posted reviews being substantially more positive than if the marketer had not engaged in the practice.

q. **Ranking by third-party review site and paid ranking boosts:** A site that provides rankings of various manufacturers' products and accepts payments in exchange for higher rankings is deceptive regardless of whether the website makes an express claim of independence or objectivity. There is also potential liability of a manufacturer that pays for a higher ranking. If a manufacturer makes payments to the review site but not for higher rankings, there should be a clear and conspicuous disclosure regarding the payments, with a cross-reference to an example involving payments for affiliate links.

r. **Requirement of disclosure of material connections:** Advertisers must disclose connections between themselves and their endorsers that might materially affect the weight or credibility of the endorsement (i.e., the connection is not reasonably expected by the audience). The disclosures must:

– Be clear and conspicuous. The proposed revisions add a definition of that phrase (as discussed above), and delete the more ambiguous statement that such disclosures must be "fully" disclosed.

– Disclose any "material connection." Material connections can include a business, family or personal relationship; monetary payment; the provision of free or discounted products or services to the endorser, including products or services unrelated to the endorsed product; early access to a product; or the possibility of winning a prize, of being paid, or of appearing on television or in other media promotions. A material connection can exist regardless of whether the advertiser requires an endorsement for the payment or free or discounted products.

– Although the nature of disclosure does not require the complete details of the connection, it must clearly communicate the nature of the connection sufficiently for consumers to evaluate its significance.

s. **Celebrity endorsement interviews and disclosures during interviews:** A disclosure should be made during a celebrity interview because a disclosure during the show's closing credits is not clear and conspicuous. If the celebrity makes the endorsement in one of her social media posts, her connection to the advertiser should be disclosed regardless of whether she was paid for the particular post. Receipt of free or discounted services can

constitute a material connection.

t. **Reuse of a celebrity's social media post:** When reusing a celebrity's social media posts in its own social media, an advertiser should clearly and conspicuously disclose its relationship to the celebrity (assuming the initial post necessitated a disclosure).

u. **Blogger who monetizes content:** A blogger who writes independent content reviewing products and who monetizes that content with affiliate links should clearly and conspicuously disclose the compensation.

Social Media Policies Are Required, and Compliance is Mandatory

The FTC has made it clear: Social media policies are a must. As the authors have found out in defending several companies in FTC investigations, there are no exceptions for the size of the business, the product or service being sold, or the industry. Every business that engages in social media advertising must have a formal social media policy. Those policies should be implemented with management oversight and must be effective. The policies should be communicated to third-party vendors as well as employees.

The FTC expects marketers to train employees on proper social media use. This obligation may extend beyond employees to third-party agents depending on the underlying relationship between a third-party agent and the marketer. Finally, some form of monitoring is expected to ensure compliance with the marketer's social media policy and the FTC's regulations and guidance.

How We Can Help

Holland & Knight's Consumer Protection Defense and Compliance Team includes a robust social media practice, with experienced attorneys that are recognized thought leaders in the field. From representing dozens of companies and individuals in federal and state investigations concerning advertising and marketing to compliance counseling and transactional contract matters involving celebrities, the firm's practice includes regulatory, compliance, litigation, investigation and transactional work in the social media space.

For more information or questions about the specific impact that social media advertising and marketing regulations can have on you or your company, contact the authors.

Anthony E. DiResta, co-chair of the Holland & Knight's Consumer Protection Defense and Compliance Team, is an attorney in the Washington, D.C., and Miami offices. He is a nationally recognized leader in defending governmental law enforcement investigations and litigation, who has successfully defended companies and individuals in dozens of high-profile, "bet-the-company" investigations by the U.S. Department of Justice (DOJ), Federal Trade Commission (FTC), Consumer Financial Protection Bureau (CFPB), and almost all of the state attorneys general – *with many of those investigations being closed*.

202.469.5164 | Anthony.DiResta@hklaw.com

Da'Morus A. Cohen is an attorney in Holland & Knight's Miami office. Mr. Cohen is a member of the firm's Litigation and Dispute Resolution practice group and Consumer Protection Defense and

Compliance Team. Mr. Cohen focuses his practice on a wide array of consumer protection and compliance matters, including governmental investigative and enforcement proceedings, regulatory compliance, and advertising and promotional marketing compliance, including social media and digital media. Mr. Cohen regularly provides advertising counsel and regulatory advice to leading Fortune 500 and Fortune 100 companies in many different product and service categories, including telecommunications, healthcare, retailing, publishing, entertainment, social media, digital media, gaming, food and beverage, and financial services.

305.789.7426 | DaMorus.Cohen@hklaw.com

Benjamin Genn is a Washington, D.C., litigation attorney who focuses his practice on complex commercial disputes and government investigations. He is well-versed in handling matters for individuals, organizations and small to large corporations regarding regulatory issues, government enforcement, white-collar crime and antitrust issues.

202.469.5489 | Benjamin.Genn@hklaw.com

FTC Report Signals Caution On AI Tools For Online Content

By **Anthony DiResta, Kwamina Thomas Williford and Wanqian Zhang** (July 25, 2022)

Anthony DiResta

Kwamina Thomas Williford

Wanqian Zhang

An interesting report by the Federal Trade Commission, released on June 16, revealed that the agency is critical of the use of artificial intelligence to combat online harms. In fact, the agency found that the use of AI has not significantly curtailed online harms overall, and may even be creating biased and discriminatory practices.

Online harms that are of particular concern include online fraud, impersonation scams, fake reviews and accounts, bots, media manipulation, illegal drug sales and other illegal activities, sexual exploitation, hate crimes, online harassment and cyberstalking, and misinformation campaigns aimed at influencing elections.[1]

While the FTC's report recognizes AI's use in combating harmful content and other positive outcomes, it also cautions against overreliance on the technology.

While some believe that the report has shortcomings, it is nevertheless important for companies to familiarize themselves with the FTC's concerns about the use of AI, and heed its guidance.

For example, data minimization is critical. Companies should collect only the information necessary to provide the service or product to the consumer.

In addition, companies should be transparent, and provide all material information upfront to the consumer that is relevant to the nature of the transaction and the purchasing decision.

Finally, human oversight and monitoring should be enhanced. Robust complaint management and awareness of regulatory compliance developments are critical.

AI's Shortcomings, and Other Problems

The FTC report finds AI to be effective in combating harms for which detection requires no context — including illegal items sold online and child pornography — and recognizes effective AI systems in preventing the inadvertent release of harmful information.

AI can be used for intervention or friction purposes before the release of harmful content, including labeling, adding interstitials and sending warnings. But the FTC does not believe these strategies prevent maliciously spread information.[2]

Platforms can also use AI tools to address online harms by finding the networks and actors behind them. AI tools can facilitate cross-platform mapping of certain communities spreading harmful contents. However, these strategies can also inadvertently ensnare marginalized communities using protected methods to communicate about authoritarian regimes.

Notwithstanding the inevitability of AI use, the FTC is concerned with using AI to combat online harms, and cautions against overreliance on it for several reasons.

First, AI tools have built-in imprecision. The FTC report cautions that data sets used to train AI systems are often not sufficiently large, accurate and representative, and the classifications can be problematic.

The report explains that AI tools are generally deficient at detecting and including new phenomena, and the operation of AI tools is subject to platform moderation policies that may be substantially flawed. The report also suggests that AI tools are often unreliable at understanding context, and therefore typically cannot effectively detect frauds, fake reviews and other implicitly harmful contents.

The report further suggests that use of AI cannot solve — and instead, can exacerbate — bias and discrimination. It explains that inappropriate data sets and a lack of diverse perspectives among AI designers can exacerbate discrimination against marginalized groups.

The report cautions that big technology companies can influence institutions and researchers, and set the agenda for which AI research the government funds.

Additionally, the report warns that AI tools used to uncover networks and actors behind harmful contents may inadvertently stifle minority groups. The FTC's research indicates that AI development can incentivize invasive consumer surveillance — because improving AI systems requires amassing large amount of accurate, representative training data.

Finally, the report notes that bad actors can easily escape AI detection by hacking, using their own developing AI technology, or simply using typos and euphemisms. It also warns that the massive amount of ordinary and pervasive posts that express discriminatory sentiments cannot be detected effectively by AI, even under human oversight.

Proposed Recommendations

The report identifies the need to increase the transparency and accountability of those deploying AI as a top priority. It stresses the importance of increasing data and AI designer/moderator diversity to combat bias and discrimination. The report also finds that human oversight is a necessity.

Transparency

The FTC report stressed that to increase transparency, platforms and other entities should do the following:

- Make sufficient disclosure to consumers about their basic civil rights and how their rights are influenced by AI. The report points out that consumers have the right to be free from being subjected to inaccurate and biased AI, the right to be free from pervasive or discriminatory surveillance and monitoring, and the right to meaningful recourse if the use of an algorithm harms them.

- Give researchers access to sufficient, useful, intelligible data and algorithms for them to properly analyze the utility of AI, and the spread and impact of misinformation.

- Keep auditing and assessment independent, while protecting auditors and whistleblowers who report illegal AI use.

Accountability

The FTC report stressed that to increase accountability, platforms and other entities should conduct regular audits and impact assessments, should be held accountable for the outcome and impact of their AI systems, and provide appropriate redress for erroneous or unfair algorithmic decisions.

Assessing Through a Diverse Lens

The FTC report recommends increasing diversity in data sets, AI designers and moderators. Firms need to retain people with diverse perspectives, and should strive to create and maintain diverse, equitable and inclusive cultures.

AI developers should be aware of the context where the data is being used, and the potential discriminatory harm it could cause, and mitigate any such harm in advance.

Human Oversight

The FTC stresses the importance of proper training and workplace protection of AI moderators and auditors. The training should correct human moderators' implicit biases and moderators' tendency to be overly deferential to AI decisions.

The FTC encourages platforms and other internet entities to use algorithmic impact assessments, or AIAs, and audits, as well as document the assessment results in a standardized way. AIAs allow for the evaluation of an AI system's impact before, during or after its use.

Companies can mitigate bad outcomes in time with AIAs, and the FTC and other regulators can obtain information from AIAs for investigations into deceptive and unfair business practices. An audit focuses on evaluation of an AI model's output.

Criticism of the Report

FTC Commissioner Noah Phillips issued a dissenting statement, and Commissioner Christine Wilson also listed several disagreements that she had with the report in a concurring statement. The two commissioners based their criticisms on three grounds.

First, the agency did not solicit sufficient input from stakeholders. The dissenting commissioners perceive the FTC report as a literature review of academic articles and news reports on AI.

They note that the report's authors did not consult any internet platforms about how they view AI efficacy, and they find that the report frequently cites to the work and opinions of current FTC employees, holding that the quantity of self-reference calls the objectivity of the report into question.

Second, they believe that the report's recommendation might produce the countereffect of subjecting compliant entities to FTC enforcement actions.[3]

Third, they conclude that the report's negative assessment of AI use in combating online harms lacks foundation. They find that conclusions of AI inefficiency are sometimes based on the fact that harmful contents are not completely eliminated by AI tools.

The dissenting commissioners say that the report lacks a cost-benefit analysis of whether the time and money saved by using AI tools to combat harmful contents outweigh the costs of the AI tools missing some percentage of these contents.

Key Takeaways

AI has tremendous benefits that companies leverage every day. But when doing so, it is prudent to be mindful of the FTC's cautions, and take steps to fortify practices related to AI.

Data Minimization

The FTC is not against implementing innovative AI tools to prevent frauds or fake reviews. However, the agency encourages data minimization.

Companies should collect only the information necessary to provide the service or product. And companies should tailor data collection to their need to render services or products.

Transparency

The FTC may require social media platforms and other internet entities to disclose sufficient information to allow consumers to make intelligible decisions about whether to and how to use certain platforms.

The FTC may also require entities to grant researchers access to information and algorithms, to a certain extent.

Accountability

The FTC may hold platforms and other internet entities responsible for impact of their AI tools, especially if the AI harms the rights of marginalized groups — even if the tools are intended for combating harmful contents.

Human Oversight

Companies should enhance human oversight. The FTC may encourage standardization of appropriate training of AI moderators/auditors and enhancement of their workplace protection.

Consumer Privacy

Companies should take care to refrain from invasive consumer surveillance. Consumer privacy interests outweigh accuracy and utility of AI tools.

Free Speech Concerns

Companies should be cautious about potential free speech disputes when prebunking alleged misinformation.

Further Guidance

The FTC may conduct more research on using AI to combat online harms. Its guidance may be subject to significant change, based on the sources it decides to consult.

Anthony E. DiResta and Kwamina Thomas Williford are partners, and Wanqian Zhang is a summer associate, at Holland & Knight LLP.

[1] In legislation enacted in 2021, Congress directed the FTC to examine ways that AI "may be used to identify, remove, or take any other appropriate action necessary to address online harms." See Statement of Commissioner Alvaro M. Bedoya Regarding Report to Congress on Combatting Online Harms Through Innovation, FTC (June 16, 2022) (acknowledging that in the 2021 Appropriations Act, Congress asked the commission to report on the use of AI to detect or address harmful online content including fake reviews, opioid sales, hate crimes and election-related disinformation).

[2] Commissioners Christine Wilson and Noah Phillips are concerned about "prebunking misinformation" recognized as effective in the report. Both point out in their statements that prebunking information that is not verifiably false, but may be false, might create free speech issues. See Dissenting Statement of Commissioner Noah Joshua Phillips Regarding the Combatting Online Harms Through Innovation Report to Congress and Concurring Statement of Commissioner Christine S. Wilson Report to Congress on Combatting Online Harms Through Innovation, FTC Public Statements (June 16, 2022).

[3] In 2021, the FTC brought a case against an ad exchange company for violations of the Children's Online Privacy Protection Act and Section 5 of the FTC Act. The company claimed to take a unique human and technological approach to traffic quality, and employed human review to assure compliance with its policies and to classify websites. The company's human review failed. But it was only the human review that provided the "actual knowledge" needed for the commission to obtain civil penalties under COPPA. If the company had relied entirely on automated systems, it might have avoided monetary liability. U.S. v. OpenX Technologies Inc., Civil Action No. 2:21-cv-09693 (C.D. Cal. 2021).

Holland & Knight

Early Draft of California Privacy Regulations Focuses on Opt-Out Rights, Disclosures

June 1, 2022

Holland & Knight Alert

Ashley L. Shively | Rachel Marmor

Highlights

- The California Privacy Protection Agency (the Agency) released a preliminary draft of its proposed regulations implementing the California Consumer Privacy Act (CCPA) as amended by the California Privacy Rights Act (CPRA).
- The lengthy draft includes detailed requirements for obtaining and implementing consumer direction regarding the sale and sharing of personal information, but it does not cover a number of hot topics, including unique employee and business-to-business issues, retention, cybersecurity audits, privacy risk assessments and automated decision-making.
- Because the regulations already are unlikely to be finalized in advance of the CPRA's effective date of Jan. 1, 2023, businesses should begin big-picture planning now.

The newly formed California Privacy Protection Agency (the Agency) quietly released a preliminary draft of its proposed regulations on May 27, 2022, implementing the California Consumer Privacy Act (CCPA) as amended by the California Privacy Rights Act (CPRA). The 66-page draft includes seven full pages of detailed requirements for obtaining and implementing consumer direction regarding the sale and sharing of personal information, but it does not cover a number of privacy hot topics mentioned in the grant of rulemaking authority to the Agency.

The Agency is required to conduct a formal notice and comment process on the proposed regulations, creating a strong probability of future changes. However, some of the more complicated proposed obligations – particularly around opting-out of sales and sharing – will require significant preparation, planning and budget to implement. Because the rules already are unlikely to be finalized in advance of the CPRA's effective date of Jan. 1, 2023, businesses should begin big-picture planning now.

Range of Topics Covered

View larger image

The draft regulations do not set forth any particular rules related to handling of personal information relating to or privacy requests from employees or individuals who interact with a business in a business capacity. They also do not elaborate on the new requirement for a business to make disclosures in its privacy policy about its practices related to retention of personal information or other topics set out in the grant of rulemaking authority [Civ. Code § 1798.185(a)], including cybersecurity audits, privacy risk assessments and automated decision-making.

Key Takeaways

It will take substantial time for business and legal teams to fully digest the implications of this lengthy draft and begin to strategize on a plan to operationalize concepts while still leaving flexibility for inevitable changes before the regulations become final. On first read, however, some themes and likely operational challenges emerge:

- **Heavy focus on consumer-friendly presentation of privacy options.** The draft rules push a detailed vision as to how a consumer should experience the process of making privacy choices, including requiring that the process be "easy to understand," prohibiting "dark patterns," requiring "symmetry in choice" and prohibiting manipulative language. This would create significant leeway for the Agency to bring actions against businesses based on subjective judgments about their websites. Further, businesses are likely to experience tension between this principle and the complex requirements related to website disclosures and pop-ups discussed below.
- **Rules of the game driven by consumers' expectations.** Businesses would be restricted to using personal information in a manner "consistent with what an average consumer would expect," but the proposed rules shed little light on how average consumer expectations should be determined. Some illustrative examples suggest – but do not explicitly state – that expectations would be determined by the nature of the products and services the business provides the consumer, meaning that disclosing a data processing practice in a privacy policy would not be enough to create an expectation if the processing is not essential to the provision of the product and service.
- **Confusion as to whether the law is opt-out or opt-in.** The CCPA/CPRA is an opt-out law; consent is only required for the sale or sharing of personal information related to consumers under age 16 or a secondary use not disclosed at the time of collection. But, the proposed rule that would require "collection, use, retention, and/or sharing" to be reasonably necessary and proportionate to achieve the purpose(s) for which the personal information was collected or processed" seems to require opt-in consent for many collections of sensitive personal information and sales of personal information. Examples offered to demonstrate the rule suggest that explicit consent would be required for collection of geolocation information through a mobile app, sale of geolocation information and disclosure of a customer mailing list in a way that it would be used for marketing of other companies' products and services. This interpretation has significant implications; it is hard to see how most, if not all, sales of personal information could be "necessary" to providing the products and services.
- **Website user experience likely to become more clunky.** Various provisions would require new popups, links and disclosures that are likely to substantially alter the user experience on websites and in stores – and many of these features nudge the legal framework toward opt-in. For example, while there is no requirement in the CCPA/CPRA for a business to request that a user accept cookies, the draft regulations call out that, under the symmetry rule, cookie banners must offer both accept and decline options. See § 7004(A)(2)(C). The business must disclose in its privacy policy how a consumer can use an opt-out preference signal [§ 7011(e)(3)(F)] and display to a user whose browser sends such a signal whether it was honored [§ 7025(c)(6)]. The requirements for offering privacy disclosures are equally detailed. For instance, the draft provides that the "notice at collection" provided at or before the point of collection cannot be satisfied by linking to the full privacy policy; a business must deep-link to the specific section of its privacy policy that provides the relevant information [§ 7012(f)], and that link must be provided "in close proximity" to the fields where information is sought or the submit button. § 7012(c)(2). These website and

disclosure requirements may effectively set national or global standards; it may not be feasible for businesses to meet these obligations just for California website visitors.

- **Enhanced downstream accountability.** Sections 7051 and 7053 describe the requirements that would apply to vendor contracts. Of note, the draft seemingly would create a new duty for businesses to conduct due diligence on service providers, contractors and third parties. 7051(e) ("[w]hether a business conducts due diligence of its service providers and contractors factors into whether the business has reason to believe that a service provider or contractor is using personal information in violation of the CCPA and these regulations."); § 7053(e) (similar). Contracts with service providers, contractors and third parties would also be required to state the "specific" purpose for disclosing the personal information, and this statement cannot be "in generic terms," which could mean that businesses must undertake significant work to update contracts. § 7051(a)(1); § 7953(a)(1).

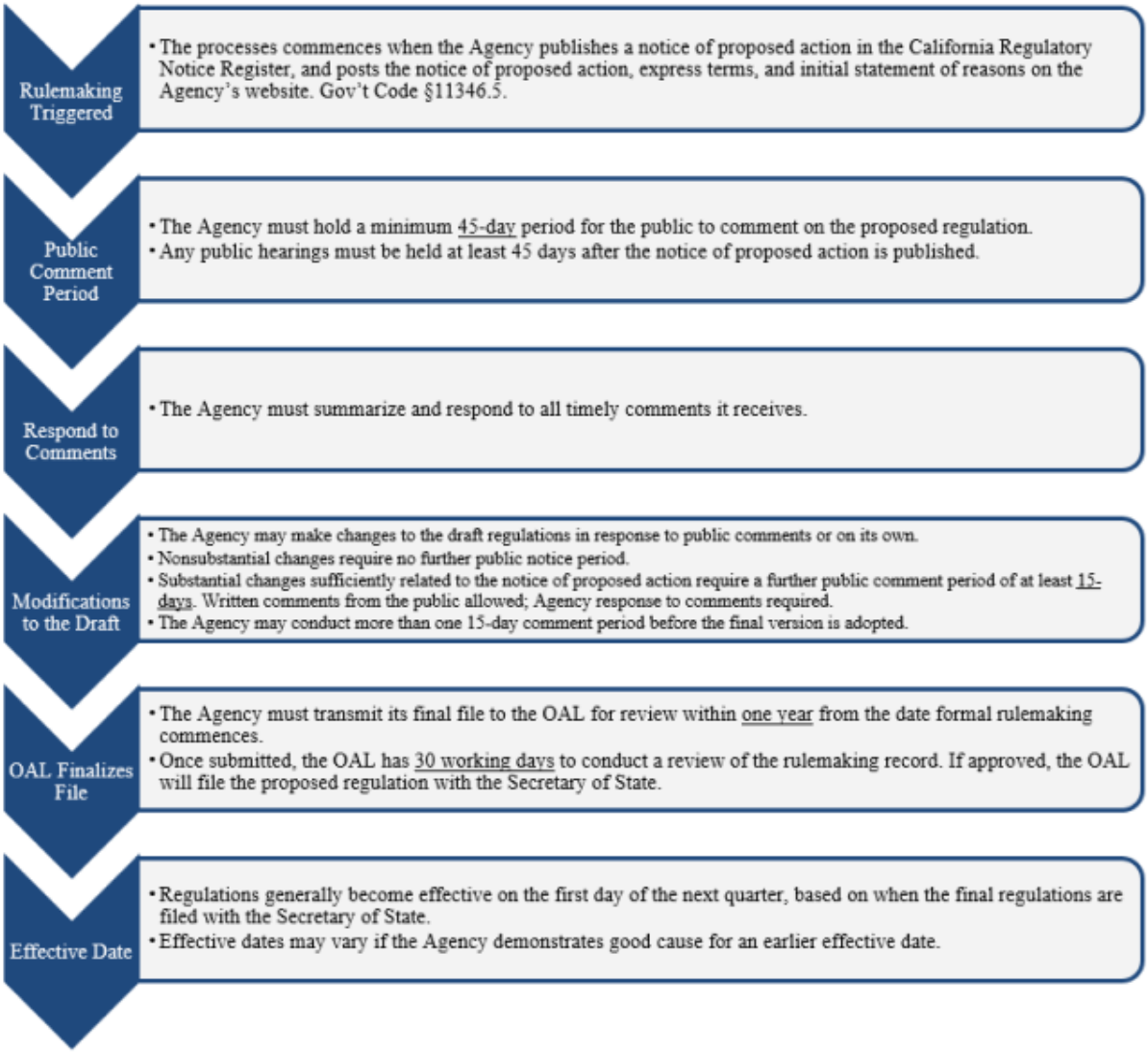
Other Noteworthy Provisions

- The draft would create new definitions for squishy terms such as "disproportionate effort" and "frictionless manner." §§ 7001(h), (k). While perhaps helpful in theory, these definitions seemingly have little grounding in actual business operations.
- Requests to opt-out of sales and/or sharing need not be verifiable and must be communicated to third parties. §§ 7026(d), (f).
- Section 7050(c) would make explicit that an entity who contracts with a business to provide targeted ads, i.e., "cross-contextual behavioral advertising," cannot be a service provider but rather is a third party, and such sharing is subject to opt-out.
- Along the same lines, a self-serve cookie management control process alone would not be sufficient to effectuate requests to opt-out of sales and/or sharing, because a cookie tool addresses sharing and not sales. § 7026(a)(4).
- Businesses would be required to list in their privacy policies the names of all third parties that the business allows to collect personal information from the consumer, which would include the names of all third parties who set cookies on the business's website. § 7012(g).
- If a business receives a request to correct information it received from a consumer data broker, it must both correct the information and ensure that it is not overridden by inaccurate information later re-received from the data broker. [See § 7023(c).] The business must also disclose the name of the data broker supplying the inaccurate information to the consumer. § 7023(i).

What Happens Next

Although the CPRA requires the CPPA to finalize regulations by July 1, 2022, the state's protracted rulemaking process means final regulations are unlikely until January 2023, if not later. The Agency's next public meeting is scheduled for June 8, 2022, and it has listed discussion of the draft regulations on the agenda.

Holland & Knight



View larger image

How We Can Help

If you have any questions about the draft regulations and the potential impact to your business, please contact the authors.

Ashley L. Shively is a privacy attorney and class action litigator in Holland & Knight's San Francisco office.

Holland & Knight

Ms. Shively counsels public and private companies on consumer protection and data privacy issues with respect to product development, sign-up and point-of-sale procedures, digital marketing, regulatory compliance, incident response, and state and federal enforcement. She regularly advises on the Children's Online Privacy Protection Act (COPPA), Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003, Fair Credit Reporting Act (FCRA), Gramm-Leach-Bliley Act (GLBA), state privacy and unfair and deceptive practices laws, and similar legal and regulatory requirements. At present, she is particularly focused on the comprehensive privacy laws enacted in California, including the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA), as well as analogous laws passed in Colorado (Colorado Privacy Act, or CPA) and Virginia (Consumer Data Protection Act, or CDPA) and similar legislation under consideration in other states.

415.743.6906 | Ashley.Shively@hklaw.com

Rachel Marmor is a privacy attorney in Holland & Knight's Boston office. Ms. Marmor counsels clients on a range of legal issues related to data strategy, consumer and employee privacy compliance, transaction risk and emerging technologies.

617.854.1436 | Rachel.Marmor@hklaw.com

Holland & Knight

Colorado Releases Proposed Privacy Rules, Further Complicating National Compliance Landscape

October 4, 2022

Holland & Knight Alert

Rachel Marmor | Ashley L. Shively

Highlights

- The Colorado Department of Law issued proposed rules to implement the Colorado Privacy Act (Draft CO Rules) on Sept. 29, 2022, foreshadowing additional compliance obligations for businesses that engage with Colorado residents online or offline.
- The Draft CO Rules stand in stark contrast to the underlying law, which is high-level and largely follows the Virginia Consumer Data Protection Act (VCDPA).
- Though the Draft CO Rules are not as proscriptive as the proposed California Consumer Privacy Act (CCPA) rules regarding consumer-facing requirements, the Draft CO Rules would impose new requirements around data governance and management of sensitive data.

The Colorado Department of Law filed a set of proposed rules to implement the Colorado Privacy Act (Draft CO Rules) on Sept. 29, 2022, foreshadowing additional compliance obligations that businesses will have to strive to meet in 2023. The level of detail in the document – which is nearly 40 single-spaced pages in 10-point font – stands in stark contrast to the underlying law, which is high level and largely parrots the Virginia Consumer Data Protection Act (VCDPA). Though the Draft CO Rules are not as proscriptive as the proposed California Consumer Privacy Act (CCPA) rules regarding consumer-facing requirements, the Draft CO Rules focus much more heavily on data governance and management of sensitive data.

Because the Colorado Privacy Act does not go into effect until July 1, 2023, the rules are not on track to be finalized until sometime in the first half of 2023. However, businesses will likely need to immediately assess how the obligations fit into their compliance roadmap in light of ongoing work to comply with VCDPA and the California Privacy Rights Act (CPRA) amendments to CCPA, by Jan. 1, 2023 – both of which cover many of the same topics. Many of the proposed requirements of the Draft CO Rules are likely to take significant time to implement, particularly the data management requirements, which may have a tail of a year or more. To add to the complications, the timing of the final CCPA Rules is entirely uncertain, as the California Privacy Protection Agency (CPPA) already missed the July 1, 2022, statutory deadline for finalization.

Key Takeaways

- The Draft CO Rules are meaty, covering a range of topics in complex detail, from consumer-facing compliance (disclosures, handling requests and opt-out mechanisms), handling sensitive data, data minimization and purpose limitations, data protection impact assessments and restrictions related to profiling.
- The language of the Draft CO Rules is softer than the CCPA Rules – a number of rules are phrased as "may" instead of "must." But they also contain different rules for different permutations of situations – for example, one set of requirements for a pre-opt out from profiling disclosure, and another set of requirements for seeking consent for profiling after an opt-out.

- The Draft CO Rules would create a new class of "Sensitive Data Inferences" and add extra restrictions to the collection, creation and processing of such data.
- The Draft CO Rules contemplate a framework for data management wherein the organization has, in a centralized function, a detailed understanding of the ways in which data is collected, used and disclosed.

Analysis

The consumer-facing compliance requirements draw heavily from the draft CCPA Rules.

The Draft CO Rules contain a number of specifications to ensure that required disclosures are consumer-friendly, such as requirements to avoid legal jargon, publish disclosures in the languages in which the controller ordinarily does business and make disclosures accessible to consumers with disabilities (Rule 3.02(A)) – all requirements of the CCPA Rules. The requirements for submission of consumer requests do not materially differ from the CCPA Rules either (Rule 4.02). Two new aspects of the Draft CO Rules: a requirement to provide data in response to an access request in the language in which the consumer interacts with the business (Rule 4.04(c)(2)) and permission to direct consumers to self-service correction options (Rule 4.05(B)).

The Draft CO Rules take a slightly different approach to universal opt-out mechanisms.

Like the CCPA Rules, the Draft CO Rules devote a lot of text to the concept of an opt-out preference signal that is automatically communicated to businesses. The approach differs in a few material ways from the CCPA Rules, however. The Draft CO Rules contemplate that the Colorado Department of Law will issue a list of approved mechanisms – whereas the CCPA Rules would require recognition of any signal that is commonly recognized and indicates an intent to opt out. The Draft CO Rules also contemplate that a universal opt-out mechanism may be a "do not sell list" that businesses query on a regular basis – perhaps similar to how national and state Do Not Call Lists under the Telephone Consumer Protection Act (TCPA) operate.

Rules on purpose specification and data minimization would require granular tracking of processing activities.

The Draft CO Rules seem to require something more than the standard "How We Use Your Information" section in a privacy policy. Businesses would be required to "specify the express purposes" for which data is collected and processed in terms that are "sufficiently unambiguous, specific, and clear" such that they can be understood by the "average Consumer" and "enforcement authorities" (Rule 6.06). Businesses would also be required to conduct and document a "data minimization" analysis of each processing activity to assess whether the activity meets the requirement to use only the minimum personal information necessary, adequate and relevant for the express purpose (Rule 6.07).

Strict restrictions would apply to the processing of "Sensitive Data Inferences."

The Draft CO Rules create a new concept called "Sensitive Data Inferences," which are inferences that indicate an individual's racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life or sexual orientation, or citizenship or citizenship status (Defined Terms at 2.02). Businesses must obtain consent to process Sensitive Data Inferences (Rule 6.10(A)), unless a four-part test is met:

1. the purpose of the processing is obvious to a "reasonable Consumer"
2. both the underlying personal data and the Sensitive Data Inferences are deleted within 12 hours of collection or completion of the processing activity
3. the data is not sold or even shared with any processors
4. the data is not processed for any secondary purpose (Rule 6.10(B))

If the business will collect consent – which almost all will – the Draft CO Rules set forth extensive requirements for consent (Rule 7), including that it must be refreshed at regular intervals (Rule 7.08).

DPIAs must be a "genuine, thoughtful analysis" of risks and benefits.

The Colorado Privacy Act requires that businesses conduct a "data protection impact assessment," (DPIA) where a processing activity presents a "heightened risk of harm." Colo. Rev. Stat. 6-1-1309(1). Rule 8.04 of the Draft CO Rules sets forth 18 pieces of information that must be included in the DPIA and offers 11 different privacy risks that businesses must consider. The DPIA must be updated regularly throughout the time the processing activity is conducted – at least annually if the DPIA relates to Profiling in furtherance of "Decisions that Produce Legal or Similarly Significant Effects Concerning a Consumer" (Rule 8.05). While the Colorado Privacy Act does not require retroactive DPIAs for processing activities commenced before July 1, 2023, the Draft CO Rules would effectively eviscerate that exception by treating an activity as "new" if changes are made in the way an internal system handles personal data or a processor is changed (among other triggers) (Rule 8.05(D)).

Profiling

If a business uses automated processing to further "Decisions that Produce Legal or Similarly Significant Effects Concerning a Consumer," it must designate a method for individuals to opt out of such decisions (Rule 9.04(D)). The business must also provide the consumer with a notice that includes a "plain language explanation of the logic used in the Profiling process" and whether the system has been evaluated for "accuracy, fairness, or bias" (Rule 9.03(A)). The business can deny a request to opt out if there is human involvement in the automated processing, but if it does, it has to provide another notice (Rule 9.04).

What Happens Next?

A number of stakeholder hearings have been scheduled for November 2022 on different topics covered by the Draft CO Rules, and stakeholders can also submit written comments. A full public hearing has been scheduled for Feb. 1, 2023 – meaning that it will be several months before there is clarity as to what will be included in the final rules.

If you have questions about the potential impacts to your business, please contact the authors or another contact the authors or another member of Holland & Knight's Data Strategy, Security & Privacy Team.

Rachel Marmor is a privacy attorney in Holland & Knight's Boston office. Ms. Marmor counsels clients on a range of legal issues related to data strategy, consumer and employee privacy compliance, transaction risk and emerging technologies.

617.854.1436 | Rachel.Marmor@hklaw.com

Ashley L. Shively is a privacy attorney and class action litigator in Holland & Knight's San Francisco office.

Ms. Shively counsels public and private companies on consumer protection and data privacy issues with respect to product development, sign-up and point-of-sale procedures, digital marketing, regulatory

Holland & Knight

compliance, incident response, and state and federal enforcement. She regularly advises on the Children's Online Privacy Protection Act (COPPA), Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003, Fair Credit Reporting Act (FCRA), Gramm-Leach-Bliley Act (GLBA), state privacy and unfair and deceptive practices laws, and similar legal and regulatory requirements. At present, she is particularly focused on the comprehensive privacy laws enacted in California, including the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA), as well as analogous laws passed in Colorado (Colorado Privacy Act, or CPA) and Virginia (Consumer Data Protection Act, or CDPA) and similar legislation under consideration in other states.

415.743.6906 | Ashley.Shively@hklaw.com

Holland & Knight

California AG Assesses First CCPA Penalty, Announces New Enforcement Examples

August 25, 2022

Holland & Knight Cybersecurity and Privacy Blog

Rachel Marmor | Ashley L. Shively

California Attorney General (CA AG) Rob Bonta announced on Aug. 24, 2022, that his office had reached a settlement with Sephora Inc. (Sephora) to resolve claims that the manner in which Sephora used third-party tracking technologies violated the California Consumer Privacy Act (CCPA). The action is the first formal complaint brought by the AG under the CCPA, which became effective on Jan. 1, 2020. If approved, the settlement will require Sephora to take immediate action to comply with the law, conduct regular compliance assessments for two years and pay a $1.2 million fine.

The Allegations Against Sephora

The complaint alleges that Sephora installed certain analytics and advertising cookies and other tracking technologies on its website and mobile apps that enabled the providers of those technologies to track the activity of Sephora users, including on products viewed or items added to carts. Those third-party providers then matched the user activity collected from Sephora's website and apps with data they collected from other sources to assist Sephora in identifying customer targets and serve advertising to them on other internet properties. The nature of the products sold by Sephora meant that the third parties could infer information about an individual that might be considered highly personal – for example, the third party would know that an individual had purchased prenatal vitamins from Sephora.

Though Sephora took the position in its website privacy policy that the company did not "sell" personal information, the AG's office argues in the complaint that allowing third parties to collect personal information via cookies was in fact a sale of that personal information. This sale triggered obligations for Sephora to offer consumers the choice to opt out of such disclosures. Sephora violated the CCPA, according to the AG, first in that it failed to post a "Do Not Sell My Personal Information" link on its website and mobile apps that could be used by consumers wishing to opt out, and second in that its website did not detect and process opt-out signals sent by browsers where the user had enabled Global Privacy Control (GPC).

Sephora could not claim that the advertising and analytics partners were service providers – which would have rendered the disclosures not a sale – because it did not have "valid" contracts in place with such partners that met the requirements set forth in the CCPA for a service provider contract. The complaint does not name the third parties whose cookies were running on Sephora's website.

The Enforcement Action

According to the complaint, the CA AG identified an initial potential violation of the law by Sephora through an "enforcement sweep" of large retailers that started with an analysis of whether their websites honored GPC. This led the CA AG to dig deeper into Sephora's privacy notice and opt-out processes, during which surfaced additional issues. Sephora was notified of these violations and failed to cure them within 30 days.

In addition to claiming violations of the CCPA and its implementing regulations, the complaint includes a count for violation of California's Unfair Competition Law, alleging that Sephora's privacy policy had false or misleading statements and that consumers were deprived of their ability to opt out of the sale of personal information.

In addition to website and mobile app remediation and the monetary fine, the settlement requires Sephora to conduct annual assessments of whether it is effectively processing consumer requests to opt out of the sale of their personal

information for a period of two years and to submit such assessments to the CA AG's office. Sephora must also document the entities with whom it shares personal information and, if it takes the position that such are service providers, confirm in a report to be provided to the CA AG that appropriate contract provisions are in place.

Additional Enforcement Examples

As we reported in a previous Holland & Knight post, "California Attorney General Previews Enforcement Strategy," the AG first published examples of its enforcement activities in July 2021 – around the same time the complaint indicates Sephora was put on notice of its alleged violations.

In conjunction with the announcement of the Sephora settlement, the CA AG's office updated its public list of examples of instances in which notices of noncompliance with the CCPA were issued. Of the 13 examples provided, 10 involved some sort of failure to properly offer consumers the right to opt out of the sale of their personal information. Some alleged failures were total – the business failed to post the required opt-out link and/or honor GPC. Others related to the manner in which the opt-out choice was presented – for example, the businesses' presentation of options was confusing or forced the consumer to take extra steps, or the business failed to accept requests from authorized agents. Several examples also cited deficiencies in privacy notices, such as incorrect or misleading statements about the business's practices related to sale of personal information and/or the process to submit right to know or delete requests, such as the failure to offer two designated methods or describe the request verification process. Two examples cited failure to provide training to employees who handled consumer privacy requests.

Takeaways

- The deployment of third-party cookies and pixels on a website to collect information about a visitor's activities on the website will likely be viewed by the CA AG as a sale of personal information to the third party, subject to opt-out requirements. While a business may be able to avoid offering an opt-out by treating the party as a service provider, a legally compliant contract restricting the use of the personal information must be in place for this to work. The Sephora complaint suggests the CA AG is (at a minimum) skeptical of the standard contract terms that come with "widely available advertising and analytics" tools. Businesses, particularly online retailers, should therefore have a detailed understanding of the data flows that occur on their online properties and the ways in which third parties are using data collected.
- The CA AG believes that honoring signals sent by browsers using GPC is a requirement of current state law. Even if this is an aggressive reading of law,[1] widespread adoption of GPC is clearly expected by the California Privacy Rights Act effective Jan. 1, 2023, and seems to be required by new privacy laws in Colorado and Connecticut in coming years. Businesses that have not already moved to adopt the standard should do so.
- Missteps in the presentation of consumers' rights processes – either right to know/delete or opt-out – are easy for a regulator to identify. Once a potential issue is on the regulator's radar, it can lead to a thorough investigation of a business's privacy program, which may result in the identification of more significant issues.

Notes

[1] A global opt-out is not mentioned in the CCPA and required under the CPRA amendments to the statute only if a business does not want to provide a Do Not Sell link for opt-outs from sales of personal information.

Rachel Marmor is a privacy attorney in Holland & Knight's Boston office. Ms. Marmor counsels clients on a range of legal issues related to data strategy, consumer and employee privacy compliance, transaction risk and emerging technologies.

617.854.1436 | Rachel.Marmor@hklaw.com

Holland & Knight

Ashley L. Shively is a privacy attorney and class action litigator in Holland & Knight's San Francisco office.

Ms. Shively counsels public and private companies on consumer protection and data privacy issues with respect to product development, sign-up and point-of-sale procedures, digital marketing, regulatory compliance, incident response, and state and federal enforcement. She regularly advises on the Children's Online Privacy Protection Act (COPPA), Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003, Fair Credit Reporting Act (FCRA), Gramm-Leach-Bliley Act (GLBA), state privacy and unfair and deceptive practices laws, and similar legal and regulatory requirements. At present, she is particularly focused on the comprehensive privacy laws enacted in California, including the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA), as well as analogous laws passed in Colorado (Colorado Privacy Act, or CPA) and Virginia (Consumer Data Protection Act, or CDPA) and similar legislation under consideration in other states.

415.743.6906 | Ashley.Shively@hklaw.com