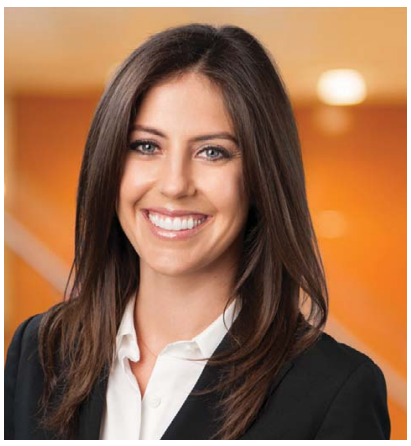
CUSTOM CONTENT

FEBRUARY 24, 2020

Data Privacy, Retail & Consumer Goods

A Roundtable Discussion



JEFFREY R. GLASSMAN
Partner, Privacy and Data Security
Ervin Cohen & Jessup LLP

STEPHEN NEWMAN AND QUYEN TRUONG
Partners
Stroock & Stroock & Lavan LLP

KATY SPILLERS
Partner
Greenberg Glusker LLP

With the emergence of the California Consumer Privacy Act, the topic of data privacy has been heating up and has clearly become one of the key focal points for success among the retail and consumer goods sectors, among the fastest growing and most vibrant business sectors in Southern California. With constantly evolving laws, regulatory protocols, best practices, consumer and business needs and industry trends seemingly changing by the season, it is sometimes hard to keep track.

To take a closer look at how the Data Privacy, Retail & Consumer Goods landscape is shaping up in 2020, and the role data privacy plays and will continue to play moving forward, we asked some of the subject's top experts in the region to share their thoughts with us.

Before getting into a deep dive on CCPA, let's take a look at the current landscape for retail and consumer goods in general. What sectors within consumer products are performing particularly well right now and why?

SPILLERS: Brands that are focused on "clean" ingredients, sustainability, and health and wellness, seem to be attracting both investment dollars and loyal customers. That being said, there are definitely challenges — managing cost of goods/margin while staying true to brand values and avoiding becoming too niche—to name a few.

What are some of the best ways for a retailer to build its brand and elevate itself from the competition?

GLASSMAN: In order for retailers to continue to build their brands in a positive light as we enter this new era of regulation over personal information, they must embrace privacy laws, educate consumers about their rights, and empower individuals to flex their muscle and exercise control over their data. Digital advertising is irreplaceable as it provides retailers with the ability to micro-target specific audiences based on their online behavior. Therefore, retailers need to adapt brands for a future of enhanced data privacy, and embrace their new partnership with consumers. A retailer's preparedness and compliance with the evolving body of privacy regulations should be part of its marketing to consumers. Acquisition costs may increase, but showing a deep-seated commitment to consumer privacy could ultimately result in a more profitable, long-term relationship with such consumers. Retailers can distinguish themselves by giving consumers reasons to opt-in to customized messaging. Successful brands will need to get creative in expanding the scope and value of their product and service offerings and use their sensitivity to protection of personal information to help shape the way their audiences interact with their brands. Telling a compelling story about a brand will no longer be adequate. The next generation of truly successful brands will return to their roots and refocus on building true brand loyalty in a more traditional sense. Retailers who invest more in understanding the full context of their consumers' lives rather than mere data points will identify the non-digital circumstances and situations that truly influence the way consumers exercise their purchasing power.

What are we seeing on the M&A front in consumer products?

SPILLERS: Large, established brands are still looking to acquire talent and innovation through acquisition. Although strategic buyers have historically been the most likely exit partners, they will continue to face competition from financial buyers, mainly private equity funds. I'm seeing funds with longer life cycles who are willing to make longer term bets and therefore behaving more like a strategic buyer in the M&A context. These funds are also reaching out to "off-market" targets and have dedicated business development colleagues who are often more nimble and adept at reaching a target before talks with a strategic partner begin.

GLASSMAN: Businesses preparing themselves for a liquidity event need to pay special attention to the evolving body of privacy laws including, but not limited to, the CCPA in order to navigate complexities, avoid traps and minimize risk. Purchasers of consumer products and services businesses often assume the liabilities of the target company including the target's failure to comply with privacy rules and regulations. As a result, privacy law compliance as part of due diligence is taking on a heightened level of importance in M&A transactions. Parties need to understand which federal, state (CCPA), and foreign (GDPR) privacy laws apply to the target's business. Buyers and sellers need to be better prepared to ask and answer privacy-related inquiries: Are the target's privacy policies adequate, transparent, complete, and accurate? Has the target complied with its own published privacy policies? What about the target's vendors, partners, subsidiaries? Are all of the target's affiliates in compliance with applicable privacy laws? What personal information is collected? What are the commercial and business purposes for which consumers' personal information is being used? What are the categories of third parties with whom the target has shared consumers' personal information? When reviewing the contracts of the target, a buyer should evaluate indemnification obligations and the extent to which its liabilities under such contracts may be inflated or limited. What kind of data security measures and information technology infrastructure does the target have in place? Representations and warranties regarding "general compliance with laws and regulations" are no longer enough. Ultimately, more specific language and detail-oriented provisions related to privacy law compliance must be included in purchase and sale agreements in order to adequately address and assess post-closing liabilities.

What does the California Consumer Privacy Act going into effect mean for consumer goods and retail businesses in 2020?

NEWMAN & TRUONG: If you have California consumers, employees, or prospects like website visitors, you need to think about how the CCPA will affect your business. Even if you do not have those California contacts, you need to think about the CCPA if you have business relationships with companies that do. If you have any type of information that could reasonably be associated with a California resident, household or device, the California Attorney General potentially can seek large penalties against you for failing to build the compliance structures necessary to give consumers various required privacy notices, protect their data from unauthorized access, and respond to consumers' exercise of their rights under the CCPA to know the pieces of their data that you have, to request deletion of certain data, and to opt out of data sales.

GLASSMAN: The CCPA means that consumer goods and services may become more expensive. The disclosures that companies need to make and the privacy-related organizational and technological infrastructure they need to implement, update, and manage could cost businesses in excess of $50 billion. Typically, those additional costs of goods and services sold find their way back to the consumers purchasing them. Under the CCPA, retailers have had to pay to update their privacy policies to disclose exactly the kind of information they are collecting about consumers, the sources that information is coming from, the retailer's commercial purpose for collecting such information, and the categories of third parties they shared consumers' personal information with. A consumer can now ask to access their personal information, that their personal information be returned to them in a form they can use to transfer such information to a different company, or that their personal information be deleted altogether. Retailers are paying for more robust and costly data security measures to protect consumers' personal information. Retailers also need to train their personnel to be in a position to understand and comply with all of the new regulations under the CCPA. All of the aforementioned will, ultimately, increase overhead and, therefore, consumers may end up paying for this new era of transparency in privacy law.

Does CCPA apply to companies that are not consumer facing?

NEWMAN & TRUONG: Potentially, yes. Even companies that are not consumer focused may get personal information for example, from website visitors or sole proprietorships. Also, every company that has California employees and meets the gross revenue or number of California residents test is covered by the CCPA, although some of the requirements pertaining to California employees do not go into effect until January 1, 2021. Additionally, to the extent the company handles data for other businesses that are consumer facing, it should develop CCPA compliance capability. At a minimum, it can expect to see contractual provisions from its consumer-facing business partners, seeking the assurances they need for their own CCPA compliance.

Does CCPA apply to all companies?

NEWMAN & TRUONG: Many small businesses are exempt, but even they may face requests from their larger business partners to comply with the CCPA. As a practical matter, they likely would be required by contract to build and implement CCPA-compliant policies and procedures. Also, the small business exemptions are narrow. To be exempt, a business must have $25 million or less in gross revenue, AND must not buy, receive or share for commercial purposes the personal information of 50,000 or more California consumers, households or devices (even just from tracking website visitors, for example). Additionally, a business OF ANY SIZE that derives 50 percent or more of its annual revenues from selling California consumers' personal information must comply with the CCPA. Notably, although the CCPA was not intended to apply to non-profits, if a non-profit engages in commercial activity (for example, through the online sale of merchandise), it may be subject to CCPA requirements.

What are the most important first steps for businesses starting to look at to in CCPA compliance?

GLASSMAN: Businesses subject to CCPA compliance must do a data collection analysis in order to determine what personal information they collect from consumers and implement an adequate information management program. Internally, the executive in charge of privacy compliance should interview the information technology department, sales personnel, customer service, legal, financial, and human resources to fully understand the scope of personal information collection and use. Externally, businesses should contact all of their key vendors and partners with which they share personal information to find out how such third parties are handling the personal information being shared with them and ensure that they are in compliance with the CCPA. Throughout this process, businesses should be classifying the different categories of personal information they collect, share or sell; organizing such information into different levels of sensitivity; determining which individuals will have access to such information based on level of sensitivity; assess adequacy of data security based on sensitivity; document data flows so personnel can visualize how personal information is handled throughout its lifecycle by the business; and determine and allocate employees responsible for complying with the CCPA. Then businesses must update their privacy policies to provide consumers with transparency about its information management systems.

NEWMAN & TRUONG: The most important first step is to perform a data inventory. Understand what data you collect currently, what legacy data you maintain and how you collect, use, or share that data. Because one of the most important rights created by the CCPA is the consumer's right to KNOW what data is maintained about him, one of the biggest compliance challenges for an organization is to KNOW precisely everything that it has. The data inventory also should encompass anticipated future collections and uses, so as to include them in your privacy policies and disclosures. As a compliance attorney, one of the most painful phone calls to get is the one that comes a week after the privacy policy or disclosure is finalized, with a question about whether something that has been in the works (but never discussed with counsel) is compliant.

What do you anticipate will be early areas of legal enforcement and what are the deadlines on compliance?

NEWMAN & TRUONG: The CCPA came into effect on January 1, and businesses sustaining data security breaches face the immediate threat of private litigation under the statute's data security provisions. Enforcement activities by the Attorney General are anticipated to begin on July 1, although they can be based on violations that occur now with respect to most provisions of the statute. Certain provisions pertaining to employees and business-to-business transactions do not become effective until January 1, 2021. Potential areas for early activity by the Attorney General include failure to provide required privacy disclosures, failing to provide easy mechanisms for consumers to exercise their CCPA rights, or discriminating between consumers for exercising those rights (including by offering financial incentives that may not meet the Attorney General's requirements).

DATA PRIVACY, RETAIL & CONSUMER GOODS

> 'For brands that are working with endorsers, understanding FTC compliance and how to allocate risks and responsibilities between a brand and an endorsement partner is critical.'
>
> KATY SPILLERS

> 'Once a business has achieved CCPA compliance, it should ensure the integrity of its information security systems by designing and developing administrative controls including incident response procedures and training.'
>
> JEFFREY R. GLASSMAN

What steps and tech compliance measures should your company take after achieving compliance with CCPA?

GLASSMAN: Once a business has achieved CCPA compliance, it should ensure the integrity of its information security systems by designing and developing administrative controls including incident response procedures and training, and implementing technical controls such a firewalls, antivirus software, and access logs. Compliance is just the first step. Thereafter, a business needs to designate an employee who will be responsible for information security; draft a list of anticipated risks to personal information, and take appropriate steps to mitigate such risks; develop security program rules, and impose penalties for violations of such rules; prevent access to personal information by former employees, and restrict overall access to records containing personal information; contractually obligate third-party service providers to comply with the CCPA; establish protocols for monitoring the effectiveness of security programs, document responses to incidents, and review the company's data security program at least once per year. There are a variety of data breach incidents businesses need to be aware of including unintended disclosures, hacking or malware, payment card fraud, insider breach, physical loss, and lost or stolen portable or stationary devices. The business must also become familiar with the fundamentals of incident management, data breach protocols, and breach notification laws. When an incident occurs, a company must first determine whether a breach actually occurred and, if so, engage in containment and analysis of the incident. Then it must notify the affected parties including individuals and government authorities, if any, and evaluate compliance with both state and federal data breach laws. Finally, for purposes of organizational learning and prevention, the company should implement effective follow-up methods like training, self-assessment, and third party audits.

NEWMAN & TRUONG: It is essential to have a program for compliance, training, and data disposal to keep a firm grasp on what and how data is being collected, maintained, used, sold or shared. This is an important step in assuring that disclosures are up-to-date and your responses to consumer requests (to know, to delete or to opt out from the sale of their data) are accurate and compliant. Companies also must be able to respond promptly to those consumer requests, as that is an ongoing compliance obligation. Finally, it is important to keep data breach protection to industry standard, because the CCPA creates significant litigation risk in the event of a data security breach.

What happens if companies don't comply with CCPA?

NEWMAN & TRUONG: The potential consequences for non-compliance are severe. The Attorney General may recover up to $2,500 per violation and up to $7,500 for each intentional violation. These penalties are on top of any penalties that might be recovered pursuant to other statutes, such as the Unfair Competition Law or the False Advertising Law, each of which also permit the Attorney General to recover up to $2,500 per violation. In private enforcement of the data security breach provisions, the potential damages also can be severe; prevailing plaintiffs can recover the greater of actual damages or statutory damages of between $100 and $750 for each person whose data was breached. That said, one saving grace of the statute is that it provides an opportunity to cure non-compliance before penalties or statutory damages are imposed. It is therefore vital for companies to attend to violation notices promptly to take advantage of the cure provisions.

What are the big private litigation threats posed by the CCPA?

NEWMAN & TRUONG: By its terms, the CCPA's provisions are enforceable primarily by the Attorney General, rather than by private litigants. The most severe private litigation threat arises in the CCPA's data security breach provisions, which authorize very large statutory damages awards in class actions ($100-$750 per person). To recover, a plaintiff must show that non-encrypted and non-redacted personal information was subject to unauthorized access, exfiltration, theft or disclosure, as a result of the business's failure to implement and maintain reasonable security procedures and practices. Significantly, a CCPA plaintiff does not need to establish that his data was actually misused or that he was the victim of identity theft or fraud. In addition, it's likely that the plaintiffs' bar will try to argue that consumers have a right to bring action under other California laws when a business violates other provisions of the CCPA.

How does the CCPA affect companies' relationships with their vendors, partners, clients and other third parties with which they exchange information?

NEWMAN & TRUONG: Under the CCPA, a business must have various contractual requirements with their vendors and other third parties, including to protect consumer data, to limit their collection, use and sharing of the data, and to impose equivalent obligations and training on their employees, vendors and other parties who may access the data. In addition, companies must track where their data goes and develop policies and procedures to pass through consumer requests for disclosure, deletion, etc., to all parties that might access and maintain the data, and do so within the timeframes required by the CCPA for responding to consumer requests.

Does an increased emphasis on digital marketing in recent years bring up legal issues to be wary of that haven't been considerations in the past?

SPILLERS: For brands that are working with endorsers, understanding FTC compliance and how to allocate risks and responsibilities between a brand and an endorsement partner is critical. Everything a brand does online is tracked, monitored and catalogued, so making sure there are processes in place for how your partners represent your brand and making sure consumers are aware of when something is paid vs. organic not only avoids legal problems, but can also add to the authenticity that customers are demanding.

GLASSMAN: Privacy is one of the most important issues to online consumers nowadays. As a result, businesses using digital marketing to promote the marketing, sale and distribution of their goods and services to consumers need to focus on balancing the need for maintaining privacy in their efforts to collect personal information from consumers against the value of using such information to grow sales. The good news is that a majority of consumers believe that receiving relevant offers is more important than keeping their online activity completely private. However, even these willing participants in digital marketing campaigns tend to proceed with caution and a heightened level of awareness about their rights. Businesses engaged in digital marketing campaigns need to understand that the sheer volume of IP addresses, devices, sensors, and other Internet of Things assets accessed and used by digital marketers exposes them to increased liability. To that end, participants must better understand what technologies are being used to collect, protect and manage consumer information. Moreover, consumers will come to expect the ability to control the scope of their participation in marketing campaigns, reduce the number and frequency of intrusions by digital marketers, and prevent third party intrusion as much as possible. Legal compliance when engaged in digital marketing is no longer an option; it is mandatory. And failure to comply can result in substantial sanctions under the CCPA including $7,500 per intentional violation and $750 per incident related to personal information compromised by inadequate data security.

NEWMAN & TRUONG: Yes! Digital marketing and the consumer data usage that goes with it generated huge privacy concerns that triggered adoption of the CCPA. So it's not surprising that the CCPA and similar laws target digital marketing. Digital marketing is so pervasive now that counsel may not know of all the ways that a company or its vendors and partners may drop cookies, pixel tags, etc., to track website visitors or may buy and combine consumer data to create customer profiles or business models. All those activities, from collection, to use, to sale, trigger specific compliance requirements. The passage of the CCPA and the publicity surrounding it also have made consumers more aware of their rights to opt out from these activities and more likely to exercise them. Companies also need to be mindful of incentives offered to secure consent to these activities, as the Attorney General's proposed regulations impose complex compliance obligations.

What cybersecurity and data privacy challenges are on the horizon?

GLASSMAN: Spyware, malware, computer viruses, fraud, abusive sales tactics that lure consumers to invest in bogus products or services, identity theft, spam, phishing and pharming attacks. These dark elements of web and mobile environments seem to be evolving faster and more aggressively than many of the defensive measures used by businesses and

consumers to protect themselves against them. Outsourced information technology management, data security services, web hosting, and cloud computing have all become increasingly popular as ways to reduce privacy and data-related risks. However, these all involve reliance by businesses on third party service providers. Businesses must implement data security systems based on the kinds of personal information being collected. The more sensitive the information, the more sophisticated the data security systems must be. Companies should avoid collecting any personal information they do not need; and they should hold onto information for only as long as absolutely necessary to accomplish and fulfill their legitimate business needs. Businesses need to insist on complex and unique passwords from their consumers, store those passwords securely, require changes to those passwords periodically, guard against brute force cyber-attacks, and protect against authentication bypass. When designing information technology networks, businesses should use tools like firewalls to segment the network into multiple parts thereby limiting access between computers, the network, and the Internet. Managed data security services is another way to actively monitor a network on a minute by minute basis for malicious activity. Companies need to regularly update and patch third party software in order to defend against the most current hacking attempts. Businesses need to upgrade their data security toolkit and partner with sophisticated cybersecurity service providers in order to address the challenges on the horizon.

SPILLERS: Direct to consumer brands are subject to increased scrutiny as a result of their digital imprint and reach. Transparency, authenticity, a commitment to diversity and sustainability practices are all brand values that consumers are tracking and using as markers for which brands to support. Making sure your endorsement partners share similar values (both contractually and as a matter of pre-contract due diligence) and having a social media team who can help manage issues as they arise are all critical. Brands who build community and regularly dialogue with their customers on both positive and negative issues seem to be faring well in the current marketplace.

NEWMAN & TRUONG: The original proponent of the CCPA is moving to put an expanded version of the statute on November's ballot. This CCPA 2.0 proposal includes the creation of a new government agency, the California Privacy Protection Agency, with significant enforcement powers. Among other things, the CCPA 2.0 proposal also would include more detailed privacy disclosure requirements, give consumers a new "right to correct" errors in data maintained by businesses, establish a new class of data described as "sensitive information" that would have more expansive protections, and prohibit arbitration of data security breach claims. Some or all of the concepts in this CCPA 2.0 ballot initiative might be adopted by the Legislature this year, even without action by the voters. Finally, about a dozen other states are either giving serious consideration to their own version of the CCPA, or have already enacted such laws.

What advertising and sales practices pose the biggest threat for class action suits against retailers and manufacturers of consumer goods?

SPILLERS: Almost every e-commerce company I know is dealing with ADA compliance issues as it relates to their website. Making sure your web developer has experience with these issues at the front-end and/or hiring a consultant to perform an audit to alert you to potential problems is key to avoiding the wave of lawsuits that is hitting DTC brands. And even if they aren't possible to avoid, make sure you are working with an advisor who has experience in dealing with and settling these types of matters. Similarly, if you are operating in California, understanding the impact of AB 5/Dynamex and the need to evaluate your employee vs. independent contractor practices is critical.

NEWMAN & TRUONG: Claims of deception or failure to make adequate disclosures pose a major threat. For example, a trend we have seen among members of the plaintiffs' bar is to challenge artwork or other content in marketing material and on product packaging as deceptive, even where the attributes of the product are accurately described in words. The theory is that the art and other content overshadow the formal disclosure, particularly with respect to products that might be purchased by less-sophisticated populations. These can be challenging cases to defend, because motions to dismiss or for summary judgment cannot rely just on the indisputable language of the packaging.

How significant a role has social media played in the world of retail?

SPILLERS: As the wholesale model and traditional retail continue to decline, retailers who embrace partnerships with direct to consumer brands (Nordstrom with Good American and Skims, for example) and leverage those brands strong social media presence, get the benefit of drawing online customers into their brick and mortar locations.

How can consumer products companies lead through innovation?

GLASSMAN: Whether through innovation or merely an effort to abide by the new information security paradigm, consumer products companies' will want to make use of as many data privacy tools as possible when interacting with consumers. A virtual private network ("VPN") routes all Internet traffic through a secure server that hides browsing history and geo-location data. Consumers may come to expect that companies they engage with online provide them with equivalent screening measures even in the absence of

DATA PRIVACY, RETAIL & CONSUMER GOODS

> 'It is essential to have a program for compliance, training, and data disposal to keep a firm grasp on what and how data is being collected, maintained, used, sold or shared.'
>
> QUYEN TRUONG

> 'The potential consequences for non-compliance are severe. The Attorney General may recover up to $2,500 per violation and up to $7,500 for each intentional violation.'
>
> STEPHEN NEWMAN

a VPN. In addition, there are certain privacy-focused web and mobile browsers actually built around privacy. These web browsers do not store or collect browsing data, they automatically block trackers, and upgrade to HTTPS, which is a protocol used for secure, encrypted communications over computer networks. Consumer products companies may want to consider driving their customer traffic through the more privacy-oriented browsers currently available. A domain name system ("DNS") is what translates domain names into an IP address that routers can use to send consumers to the right destination. By default, most consumers use a DNS from their Internet Service Provider ("ISP") and never bother to change their DNS settings. However, ISPs have long tracked where consumers visit online and now they can sell that information to advertisers. Consumer products companies may want to educate their customers on these matters or develop strategies to assist consumers in switching to encrypted DNS settings in lieu of the default settings made available by their ISPs. Consumer products companies will want to use messaging apps that support end-to-end encryption and prevent third-parties from reading consumer messages. Using messaging apps like Facebook Messenger means consumer messages are not encrypted and Facebook's systems actually read such messages so they can target consumers with Facebook advertising. Consumer products companies should also consider automatically prompting consumers to update and change passwords on a regular basis through advanced password managers.

What advice would you offer to an early stage manufacturer seeking growth capital?

SPILLERS: When raising growth-capital, I always encourage founders to focus on "smart" capital – in addition to money, what other capabilities or advice do you need? Are there investors who can offer you capital plus access to one or two of these other resources? Do the investors have a portfolio of brands who you can collaborate with and/or learn from? In order to facilitate investment, have your "house" in order before due diligence starts. If you have co-founders, make sure you have your business agreement in place. Make sure your brand/IP is protected and if it's not registered, be prepared to explain why you don't think that's a barrier to growth.