National Association of Attorneys General's 2023 Consumer Protection Spring Conference

June 13, 2023

On May 10–12, 2023, the National Association of Attorneys General (the "NAAG") held its Spring 2023 Consumer Protection Conference to discuss the intersection of consumer protection issues and technology. During the portion of the conference that was open to the public, panels featuring federal and state regulators, private legal practitioners, and industry experts discussed potential legal liabilities and consumer risks related to artificial intelligence ("AI"), online lending, and targeted advertising.

In this Debevoise Update, we recap some of the panels and remarks, which emphasized regulators' increased scrutiny of the intersection of consumer protection and emerging technologies, focusing on the leading themes from the conference: transparency, fairness, and privacy.

STATE ATTORNEYS GENERAL AND DEPUTIES REMARKS

Representatives from the Office of Attorneys General for Colorado, New Hampshire, New York, and Tennessee described their consumer protection priorities and the types of conduct they are currently scrutinizing.

Several common enforcement priorities emerged from their remarks. State Attorneys General are focused on elder fraud and abuse, social media's impact on minors' privacy interests and mental health, and the risks AI poses to consumers in terms of increased fraud, bias in credit transactions, and data privacy. In light of rapid developments in AI, New Hampshire's Attorney General intends to prioritize his office's resources on broadly impactful enforcement cases involving AI to which application of existing laws are clear, such as artificial intelligence's potential to automate and perpetuate bias in lending practices.

Representatives also focused on more granular issues including the regulation of deceptive claims regarding marijuana products (Colorado) and policing fraudulent practices in the solar industry, as well as predatory businesses that target military personnel (Tennessee).

PANELS AND ISSUES IN CONSUMER PROTECTION

Artificial Intelligence and Deep Fakes

A panel comprising representatives from the New Jersey State Attorney General's Office and private industry focused on legal issues arising out of AI's use to generate "deep fakes," and spoke more generally about how state regulators intend to use existing legal frameworks to address the risks posed by the rapid adoption of AI tools across industries. Kashif Chand from the New Jersey Attorneys General Office emphasized that the regulation of emerging technologies like AI is no different than the regulation of prior technological advancements. Similar to how Attorneys General Offices adapted to the proliferation of data breaches by enforcing them through their unfair and deceptive acts or practices ("UDAP") authority, regulators intend to use UDAP laws to police AI.

Transparency and Disclosure

The panel highlighted that transparency and disclosure are key issues for companies that utilize AI tools within their business lines. As AI becomes commonplace in the workplace, and can significantly affect consumers and employees, the panel emphasized that companies have a responsibility to disclose when and how they are using AI. To comply, the panel recommended that a company's disclosures be clearly understandable so that consumers are able to know what data are being collected, and how the company is handling and using that data. In order for companies to be able to provide adequate transparency regarding AI usage, companies should consider incorporating data privacy, security, and fairness concerns during product development.

Data Minimization and Anonymization

Panelists expressed concern that the extraordinary amount of data AI systems ingest and retain may be at odds with principles of data minimization and anonymization. The panel cited the FTC enforcement action against Drizly (which was not an AI case) as an example of how retention of unnecessary data may result in the imposition of significant injunctive relief on businesses and even their executives in certain circumstances. After a data breach that exposed the personal information of roughly 2.5 million consumers, the FTC and Drizly entered into a consent agreement that not only required Drizly to destroy the unnecessary data, but also ordered both Drizly and its CEO to implement an information security program and restrict the amount of data that Drizly collects on a prospective basis. Notably, these orders imposed individual liability and Drizly's CEO is therefore required to implement data security programs at any future companies for which he retains information security responsibilities and that collect consumer data from more than 25,000 individuals. Panelists remarked that similar risks are even more prevalent for AI models that ingest data and continuously learn and evolve overtime. To avoid UDAP violations, the panelists recommended that

companies engage in ongoing monitoring and evaluation of AI systems and the data underlying those systems to ensure that only necessary data are retained and used.

Panelists also expressed concerns about whether anonymizing customer data actually protects consumers' privacy interests. Panelists cited Strava's release of purportedly anonymized Fitbit data, which researchers nonetheless were able to circumvent and de-anonymize to discover and track individuals' geolocation information. Companies that may use anonymized data (and perhaps advertise that they do) should take care that the data are sufficiently obscured and cannot be traced back to individuals.

Content Labeling

The panel also discussed the threats that deep fakes presented to the public as AI-generated content is becoming nearly indistinguishable from authentic content. Deep fake technology poses a real risk of deception, as people will soon no longer be able to tell whether they are encountering AI-generated content or human-generated content. The authenticity of content has large implications for many industries, including the legal industry, and regulators stressed that companies developing these AI tools need to consider how to establish standards that protect authenticity and prevent deception. Companies that are developing or using this type of technology should consider labeling their content that is artificially generated so that it is clear to viewers what is real and what is AI-generated.

Targeted Advertising and Privacy

The panel, which included an attorney from the FTC's Division of Privacy and Identity Protection and data analytics experts, focused its attention on the use of data, particularly sensitive data, in advertising, emphasizing that whether data are deemed sensitive depends on the context in which such data are used. For example, personal information may become sensitive if it is deployed in a sensitive product or service such as certain types of healthcare products or services. Recent FTC actions have faulted companies for the misuse and sharing of consumer data to display advertisements based on customers' health information. A representative from the FTC discussed the agency's particular focus on products and services that use geo-location data, health data, and data of minors.

To mitigate risks associated with the use of sensitive consumer data, panelists recommended that companies, including advertisers, clearly and fully disclose to consumers their data collection, usage, and sharing practices. Further, companies should consider obtaining express consent from consumers for any use of sensitive data in advertising. In addition to these transparency and explainability principles, companies should consider implementing strong data governance procedures such as a written

privacy program, employee training, data minimization and retention standards, and the restriction of the use of sensitive data to the company's disclosed purpose. The panel also observed that the involvement of third parties does not relieve companies of their obligations to properly handle sensitive consumer data, and recommended companies incorporate protection of sensitive consumer information into any third-party contracts.

Online Lending

Senior Enforcement counsel at the Consumer Financial Protection Bureau (the "CFPB") and a representative from the Attorneys General Office of Minnesota noted their offices' focus on online and point-of-sale transactions. Both regulators expressed concern over the rise in point-of-sale financing, which typically requires a small down payment followed by short-term interest-free payments. The CFPB is focusing on "buy now, pay later" ("BNPL") options and the way companies market product features, disclose data protections, and encourage greater levels of debt. Because BNPL and other point-of-sale lending transactions typically are structured so the disclosure obligations of the Truth in Lending Act ("TILA") do not apply, the CFPB intends to utilize its authority to enforce the prohibition against unfair, deceptive, or abusive acts or practices ("UDAAP") under the Consumer Financial Protection Act of 2010 (the "CFPA") to regulate BNPL products.

In particular, the panelists spoke about the CFPB's recent policy statement on abusive acts or practices and highlighted key themes from recent CFPB enforcement actions focusing on business practices that allegedly obscure important features of a product or service, leverage unequal circumstances, and use dark patterns to influence consumer behavior. The regulators are concerned that the risks of incurring increased debt posed by repeat usage of BNPL products are not being clearly communicated to consumers. Companies should ensure product and service communications are clear, understandable, and easily accessible to consumers.

To subscribe to the Data Blog, please click here.

The Debevoise Artificial Intelligence Regulatory Tracker (DART) is now available for clients to help them quickly assess and comply with their current and anticipated AI-related legal obligations, including municipal, state, federal, and international requirements.

* * *

Please do not hesitate to contact us with any questions.

NEW YORK

Courtney M. Dankworth
cmdankworth@debevoise.com

Avi Gesser
agesser@debevoise.com

Samuel J. Allaman
sjallaman@debevoise.com

WASHINGTON, D.C.

Melissa Muse
mmuse@debevoise.com

Paul D. Rubin
pdrubin@debevoise.com

Jehan A. Patterson
japatterson@debevoise.com