

National Association of Attorneys General's 2022 Presidential Summit: Tech Threats and Tools

August 23, 2022

From August 9-10, 2022, the National Association of Attorneys General (“NAAG”) held its 2022 Presidential Summit to discuss the intersection between consumer protection and technology. The panels featured state law enforcement, private legal practitioners, and industry experts who covered salient and developing legal issues such as consumer privacy, artificial intelligence, and the Internet of Things. Federal regulators, including Consumer Financial Protection Bureau (“CFPB”) Director Rohit Chopra and Federal Trade Commission (“FTC”) Commissioners Alvaro Bedoya and Noah Phillips, offered their thoughts on consumer protection in the digital world.

In this Debevoise Update, we recap some of the panels and remarks, which emphasized the need for coordination between federal and state law enforcement, focusing on the themes emerging from the conference: privacy, security, and competition.

FEDERAL REGULATORS' REMARKS

FTC Commissioner Alvaro Bedoya

- Following introductory remarks by NAAG president Iowa Attorney General Tom Miller, FTC Commissioner Alvaro Bedoya gave his first major speech since assuming his position in May 2022.
- Bedoya's remarks focused on the disparities of digital life, how diverse populations are disproportionately targeted by fraudulent scams, and how certain populations do not receive the same legal and structural protections as others. For example, Bedoya commented on the reduced effectiveness of social media companies' fraud prevention tools for languages other than English. He did not limit this criticism to the private sector, noting that the government similarly lacks the capability to protect foreign-language speakers as robustly as English speakers.
- Bedoya encouraged federal action in the privacy arena, noting the [privacy bill](#) currently making its way through Congress. In line with his theme of how different

populations experience life online, Bedoya highlighted how geolocation tracking can harm vulnerable groups, such as battered women or women making choices about their reproductive health. According to Bedoya, the FTC (and the federal government more generally) needs to take greater action to update the nation's privacy laws to avoid leaving people behind.

- Bedoya encouraged state Attorneys General to enforce state privacy laws that may be analogous to or complement the FTC's options to pursue privacy violations, like its Safeguards Rule, the Fair Credit Reporting Act, and the Children's Online Privacy Protection Act ("COPPA").

FTC Commissioner Noah Phillips

- Departing FTC Commissioner Noah Phillips similarly expressed the need for the FTC and states to work together in the consumer protection arena, especially where there are localized frauds that state enforcers are better positioned to pursue.
- Commissioner Phillips shared his thoughts on privacy law by complimenting the Commission's role in enforcement and implying that the FTC should focus on the tools already available to it, such as COPPA and the FTC Act. He also touted the Commission's ability to meaningfully add to policy debates using studies.
- Commissioner Phillips expressed support for a single national privacy law standard, stating that a national law would not only ease compliance for business, but help create a clear rule for consumers to understand.

CFPB Director Rohit Chopra's Remarks

- Chopra staked out the CFPB's strong position on digital advertisers. Chopra traced the evolution from advertisers' traditional role as pure conduits for advertisements to active participants in the targeting of consumers to monetize their data and preferences. To that end, Chopra announced the [interpretive rule](#) the CFPB issued that same day, indicating that digital advertisers who are participating in the development and targeting of advertising to consumers are "service providers" subject to the Consumer Financial Protection Act's (the "CFPA") prohibition on unfair, deceptive, or abusive acts or practices ("UDAP").
- Chopra encouraged state law enforcement to be stronger and more robust and to enforce the federal consumer protection laws alongside the CFPB, contrasting this approach with past divergence between state and federal authorities' views.

PANELS AND ISSUES IN STATE-LEVEL CONSUMER PROTECTION

Privacy

- The conference's privacy panel highlighted perspectives from the Colorado and Utah Attorneys General's offices, as well as from industry and private practice. The group emphasized the differences among state privacy laws enacted around the country, a topic which Debevoise has previously [discussed](#).
- The panel expressed concerns about the draft federal privacy law making its way through Congress. As written, the law would preempt most state privacy laws, and 10 state Attorneys General have expressed the view that a national law should be a floor for privacy protections, rather than a ceiling.

Artificial Intelligence

- Issues associated with the use of artificial intelligence ("AI") received scrutiny in several forums. For example, use of AI in employment decisions is clearly on the radar of law enforcement.
- State Attorneys General likewise are employing their traditional consumer protection toolkit to pursue UDAP claims arising out of the use of AI. A panelist from the Vermont Attorney General's Office described a [recent action](#) against Clearview AI under the unfairness prong of the state's Consumer Protection Act.
- AI was also implicated in questions about competition, highlighting issues surrounding companies collecting data and tweaking their algorithms in ways that are purportedly anti-competitive.

Internet of Things

- Concerns about privacy and security converged in a discussion on the increased connectivity of consumer and industrial devices and systems that make up the Internet of Things ("IoT"). Devices like wearables collect massive amounts of consumer data, which pose important questions about who owns that data, where the data is sent, where it is stored, and what safeguards are in place to protect that data.
- Recent federal action highlights the importance of these issues, with respect to both privacy and data security. The IoT Cybersecurity Improvement Act of 2020 requires new minimum standards for federal procurement of IoT devices, which may set a floor for cybersecurity practices that incentivizes private industry to follow suit more generally. And in May 2021, President Biden signed [Executive Order 14028](#) on

Improving the Nation's Cybersecurity. Among other directives, the Executive Order requires the National Institute of Standards and Technology ("NIST") to create a labeling program to educate the public on security capabilities of IoT devices and software development practices.

* * *

Please do not hesitate to contact us with any questions.

NEW YORK



Courtney M. Dankworth
cmdankworth@debevoise.com



Eric R. Dinallo
edinallo@debevoise.com



Avi Gesser
agesser@debevoise.com



Scott M. Caravello
smcaravello@debevoise.com

WASHINGTON, D.C.



Paul D. Rubin
pdrubin@debevoise.com



Jehan A. Patterson
jpatterson@debevoise.com



Melissa Runsten
mrunsten@debevoise.com