



Big Tech & Free Speech Under the Microscope: FTC's New Direction

What Compliance Teams Need to Know About the Changing Approach to Consumer Protection & Data Privacy

The regulatory landscape is shifting as the FTC signals a return to its “bread and butter” work of fraud enforcement while continuing scrutiny of data privacy and Big Tech issues. Elizabeth Kwok, a managing director at FTI Consulting and former senior investigator at the FTC’s Bureau of Consumer Protection, examines how organizations can navigate this changing environment, particularly as states increasingly fill regulatory voids with their own enforcement actions.

This Q&A was originally published by [Corporate Compliance Insights](#).

As the FTC signals a new emphasis on fraud enforcement and less aggressive rulemaking during the second Trump Administration, its new chairman is expected to steer the agency toward addressing traditional fraud matters while continuing to focus on [data privacy](#) and Big Tech issues, particularly around free speech and alleged censorship of political viewpoints.

As federal regulatory oversight potentially decreases, individual states are increasingly filling the void with their own enforcement actions. This creates a patchwork of regulatory requirements across jurisdictions, complicating [compliance](#) efforts for organizations operating in multiple states. The situation is particularly challenging for companies handling children’s data, which face heightened scrutiny under the [Children’s Online Privacy Protection Act \(COPPA\)](#). Industry experts recommend that organizations take a proactive approach to understand the various regulatory schemes that apply to their businesses and develop strong compliance programs focused on data privacy and security.

Below is a Q&A with Elizabeth Kwok, a managing director at FTI Consulting. Prior to FTI Consulting, Kwok spent more than a decade in the federal government at the FTC and the Office of Inspector General in the Commerce Department. As a former senior investigator from the Bureau of Consumer Protection (BCP) at the FTC, Kwok led high-profile investigations into a wide range of consumer protection issues, including those involving fintech, cryptocurrencies, data privacy and security, AI, debt collection and debt relief products.

Q: As the Trump Administration continues to rollout their policies, including naming a new chair of the FTC, how has this shifted the regulatory landscape?

A: The regulatory landscape is shifting frequently in this new administration. Specific to the FTC, it seems they are headed back toward more of their “bread and butter” work, focusing primarily on fraud matters. The chairman and other commissioners have signaled a shift toward addressing the agency’s core mission of fraud enforcement and adhering more closely to traditional understandings of the FTC’s authority, with minimal new rulemaking expected. It’s likely the new chairman will be steering the agency away from pushing the boundaries of legal authority and from more novel approaches to enforcement. The chairman has expressed a continued interest in data privacy enforcement, as well as continuing to probe Big Tech matters, with an emphasis on free speech.

Q: Speaking of the FTC, the agency recently announced a [request for information \(RFI\)](#), seeking comments from the public regarding free speech on technology platforms. What do you anticipate the FTC will do with this information?

A: The new chairman has a history of scrutinizing Big Tech’s purported censorship of political viewpoints. As a result, he may pursue enforcement actions against tech companies that have implemented practices like content moderation, which the agency could deem unfair or deceptive or anti-competitive. It is also possible that this would be an area in which the agency could opt to engage in rulemaking.

Q: Without robust federal regulatory schemes, can it be expected that individual states fill this void? And if so, what are the potential challenges from operating in this type of environment?

A: It is expected that states will fill the void in terms of enforcement action; many states at this juncture have their own state privacy laws, and one ([California](#)) even has a private right of action for consumers. This individual patchwork of regulatory schemes is extremely complicated from a compliance perspective. Organizations operating in multiple jurisdictions will have to institute policies and procedures that comply with varying regulations, even when some state rules may not be fully aligned. Organizations will also face increased expenses because they may face enforcement action from multiple states, and they will have to resolve those matters on an individual basis.

Q: Where should organizations allocate their resources to align with regulatory frameworks?

A: Organizations would be well served to be proactive and seek to understand the variety of regulatory schemes that apply to their businesses. Strong compliance programs, including those covering data privacy and security, should be a strategic area, as those issues are top of mind for most regulators. Many of the agencies have expressed a willingness to work with industry to resolve identified problems, but the level of cooperation and collaboration will vary sharply depending on the state of the organization’s compliance at the time of any identified issues. If your organization deals with children’s data, for example, there is even more scrutiny with respect to your data privacy and security practices.

Q: Speaking of children’s data, the primary regulation governing the collection of minors’ personal information is the [Children’s Online Privacy Protection Act \(COPPA\)](#). What are the challenges of complying with COPPA and how can organizations meet the regulatory obligations?

A: The complexity of determining what data is subject to COPPA and what triggers compliance obligations is a significant challenge. The defining terms can be ambiguous; for example, what exactly does “directed to” mean, and how should organizations determine what data is appropriate to collect? Compliance with COPPA is complex — there are multiple avenues that organizations can take to meet requirements. For example, obtaining a “safe harbor” certification, which provides a presumption of compliance with COPPA. However, organizations should take a proactive approach in reviewing how they interact with children and the various ways they collect data.

The views expressed herein are those of the author(s) and not necessarily the views of FTI Consulting, Inc., its management, its subsidiaries, its affiliates, or its other professionals. FTI Consulting, Inc., including its subsidiaries and affiliates, is a consulting firm and is not a certified public accounting firm or a law firm.

FTI Consulting is the leading global expert firm for organisations facing crisis and transformation, with more than 8,300 employees in 34 countries and territories. FTI Consulting is dedicated to helping organisations manage change, mitigate risk and resolve disputes: financial, legal, operational, political and regulatory, reputational and transactional. FTI Consulting professionals, located in all major business centres throughout the world, work closely with clients to anticipate, illuminate and overcome complex business challenges and opportunities. © 2025 FTI Consulting, Inc. All rights reserved. fticonsulting.com