

U.S. Agencies Increase Coordination and Use of Technology to Investigate Data Misconduct

In brief

Federal regulatory agencies have prioritized enforcement efforts that target the mishandling of data by companies that store and monetize large amounts of personal or sensitive information. This issue cuts across multiple regulatory areas which has prompted increased coordination between federal agencies. Notably, on March 26, 2024, the U.S. Federal Communications Commission ("FCC"), Consumer Financial Protection Bureau ("CFPB"), and the Federal Trade Commission ("FTC"), publicized a coordinated effort to increase their technological capabilities to address privacy and competition concerns related to the use of data. At the same time, these agencies, along with the Department of Justice ("DOJ") and the U.S. Securities and Exchange Commission ("SEC"), have increased their hiring and use of technologists to investigate data misconduct and identify methods to more effectively address concerns around the use of artificial intelligence ("AI"). Against this backdrop, companies that handle large amounts of consumer data or employ AI should be on high alert for enhanced regulatory scrutiny, and the need for data governance in an interdisciplinary manner.

Contents

[Highlights](#)[In detail](#)[Takeaways](#)

Highlights

- Federal agencies are prioritizing investigations into the misuse of customer data. Numerous agencies, including the FCC, CFPB, FTC, and DOJ, are investing in emerging technology that can be used to detect regulatory violations and using these technologies in their investigations and enforcement.
- Each of these agencies have expanded their technical knowhow – hiring technologists to strengthen their capabilities and enforcing data security standards.
- Enforcement of antitrust, privacy, and other regulatory areas related to the handling of consumer data and AI will be the foundation for federal agencies' efforts seeking to regulate the misuse of data. For example:
 - FCC, CFPB, and FTC leadership have broadcasted plans to increase interagency coordination and investments to expand their technical knowhow including hiring technologists and developing detection technologies. Other initiatives undertaken by these agencies include the FCC's creation of its Privacy and Data Protection Task Force (which doubled the number of people at the FCC working on privacy enforcement), and FTC's establishment of its Office of Technology to "challenge the indiscriminate collection and monetization of consumer's data."¹
 - DOJ has announced that it too will invest more in detection technologies to support its criminal antitrust prosecutions. DOJ recently launched "Justice AI" to study ways for DOJ to utilize and deploy AI to prosecute white-collar crime, and the designation of DOJ's first Chief Science and Technology Advisor as well as a Chief AI Officer.

¹ FTC, *FTC Releases 2023 Privacy and Data Security Update*, (Mar. 28, 2024), <https://www.ftc.gov/news-events/news/press-releases/2024/03/ftc-releases-2023-privacy-data-security-update>.

- The SEC has prosecuted several offenders for data misconduct, and focused particular attention on the need for public companies to disclose the nature of their data breaches and how they use AI to address regulatory concerns.
- Companies should also expect to see increased cross-border collaboration among regulators. In addition to expanding their breadth of technical understanding, regulators at the International Competition Network ("ICN") Tech Forum discussed the need for greater international cooperation and initiatives for purposes of facilitating investigations related to the use of customer data and AI. Businesses that store and sell consumer data should therefore anticipate increased and coordinated enforcement from multiple regulators both domestically and around the globe.

In detail

In March 2024, dozens of state, federal, and foreign enforcers convened at the ICN Tech Forum, where officials discussed the value of increasing their technological capacity to tackle the misuse of data and investigate digital markets. During these discussions, representatives from the FCC and CFPB announced their agencies would formally coordinate with the FTC to increase interagency investigative and enforcement capabilities. These agencies also noted that such coordination would advance the prosecution of privacy and competition abuses within their respective jurisdictional areas. These statements highlight that the proper handling of customer data and responsible use of AI are key priorities and are top-of-mind for federal officials.

Federal agencies have also recently made significant strides to expand their technical capabilities by hiring personnel and adopting technologies specifically to improve capabilities to detect potential violations in sharing and monetization of data.

For example, in June 2023, the FCC created its Privacy and Data Protection Task Force. This task force more than doubled the personnel at the FCC working on privacy enforcement. The task force, led by FCC Enforcement Bureau Chief Loyaan A. Egal, employs a dedicated team responsible for investigating and enforcing violations of the Commission's privacy and data protection laws and rules.² At the same time, the FCC also hired more technologists who would aid in the task force's mission. When it discussed these initiatives, the FCC made clear that "[p]rivacy and data protection are critical to all Americans" and are a "top priority" for the FCC.³

Separately, in June 2023, FCC Chairwoman Jessica Rosenworcel issued a statement to the Center for Democracy and Technology Forum on Data Privacy about evolving trends and regulatory challenges related to the mishandling of customer data. Rosenworcel remarked that "monetization of data is big business The market incentives to keep our data and slice and dice it to inform commercial activity are enormous—and they are only growing."⁴ According to Rosenworcel, in reference to carriers for selling and sharing geolocation data, "[i]t is time to hold them accountable and make them pay up for this behavior We need to make clear that when you violate consumer communications privacy, there are consequences."⁵

The FCC has also issued plans to partner with state counterparts to strengthen data privacy enforcement. In December 2023, Rosenworcel issued a press release announcing that the agency's Privacy and Data Protection Task Force would coordinate with Attorneys General from Connecticut, Illinois, New York, and Pennsylvania.⁶ These are states that have traditionally been aggressive on data security investigations.

Like the FCC, the CFPB too has increased its technical capabilities and hired more technologists to work on cases involving data privacy, AI, machine learning, algorithmic discrimination, and secure data systems. CFPB Director Rohit Chopra stated at the

² FCC, *Privacy and Data Protection Task Force*, last updated Mar. 5, 2024, <https://www.fcc.gov/privacy-and-data-protection-task-force>.

³ *Id.*

⁴ FCC, *Remarks of FCC Chairwomen Jessica Rosenworcel to the Center for Democracy and Technology Forum on Data Privacy*, at 1, (Jun. 14, 2023), <https://docs.fcc.gov/public/attachments/DOC-394386A1.pdf>.

⁵ *Id.* at 3.

⁶ FCC, *FCC Privacy & Data Protection Task Force Launches First-Ever Enforcement Partnerships with State Attorneys General*, (Dec. 6, 2023), <https://docs.fcc.gov/public/attachments/DOC-398939A1.pdf>.

forum, "[f]rom cracking down on data abuses and shoddy AI to tracking Big Tech's movement into financial services, technology is fundamental to the CFPB's work."⁷

The CFPB has similarly placed considerable focus on data privacy concerns and regulating the storage, exchange, and monetization of data. For example, in April 2022, the CFPB published a statement warning financial companies that failing to safeguard consumer data may be a violation of federal consumer financial protection law. In addition, the CFPB has recently led a number of research endeavors to understand how technology advances consumer finance.⁸

In October 2023, the CFPB launched a probe into the data broker industry to determine whether it should be regulated under the Fair Credit Reporting Act ("FCRA").⁹ In its proposed outline, the CFPB indicated that it plans to use its authority to regulate data brokers through the FCRA.¹⁰ The CFPB's outline also addressed aggregated data and the use of data in targeted marketing campaigns. The CFPB explained that the new rules will limit the circumstances under which a consumer reporting agency can help third-party users market to consumers.

In addition, the CFPB initiated an investigation into the use of AI in financial institutions—specifically the use of customer service "chatbots."¹¹ The CFPB at the time took the view that the use of AI can violate federal consumer financial protection laws and raise potential threats in the form of algorithmic bias.¹²

The FTC has also repeatedly prioritized prosecution of data misuse—specifically data monetization. For example, to tackle digital markets, FTC Chair, Lina Khan, remarked at the December 2022 Open Commission Meeting that, "[FTC] technologists are central to that effort. Their expertise helps us respond to emerging technologies and evolving business practices."¹³ To scale up its technical expertise further, the FTC created the Office of Technology in early 2023. Shortly thereafter, the FTC released its 2023 Privacy and Data Security Update, during which Samuel Levine, Director of the FTC's Bureau of Consumer Protection stated that the FTC "is taking bold actions to challenge the indiscriminate collection and monetization of consumers' data . . . [and] securing meaningful remedies to protect consumers' information, rather than placing the burden on consumers to protect themselves."¹⁴

Consistent with the FTC's agenda on targeting data and privacy abuses, it has sued several companies for improperly selling consumers' personal data in the past several years. For example, in 2023, the FTC approved an order banning BetterHelp from sharing sensitive health data for advertising with Facebook and other third parties, and requiring it to pay \$7.8 million to provide

⁷ CFPB, *CFPB Joins Federal and State Agencies in Coordinated Statements on Tech & Enforcement*, (Mar. 26, 2024), <https://www.consumerfinance.gov/about-us/newsroom/cfpb-joins-federal-and-state-agencies-in-coordinated-statements-on-tech-enforcement/>.

⁸ CFPB, *Statement of CFPB Director Rohit Chopra and Chief Technologist Erie Meyer on Enhancing Agency Capabilities to Address Transformative Technologies*, (Mar. 26, 2024), <https://www.consumerfinance.gov/about-us/newsroom/statement-of-cfpb-director-rohit-chopra-and-chief-technologist-erie-meyer-on-enhancing-agency-capabilities-to-address-transformative-technologies/>.

⁹ CFPB, *CFPB Launches Inquiry Into the Business Practices of Data Brokers*, (Mar. 15, 2023), <https://www.consumerfinance.gov/about-us/newsroom/cfpb-launches-inquiry-into-the-business-practices-of-data-brokers/>.

¹⁰ CFPB, *Protecting the Public from Data Brokers in the Surveillance Industry*, (Aug. 15, 2023), https://files.consumerfinance.gov/f/documents/cfpb-data-broker-rulemaking-faq_2023-08.pdf.

¹¹ CFPB, *CFPB and Federal Partners Confirm Automated Systems and Advanced Technology Not an Excuse of Lawbreaking Behavior*, (Apr. 25, 2023), <https://www.consumerfinance.gov/about-us/newsroom/cfpb-federal-partners-confirm-automated-systems-advanced-technology-not-an-excuse-for-lawbreaking-behavior/>.

¹² CFPB, *Director Chopra's Prepared Remarks on the Interagency Enforcement Policy Statement on "Artificial Intelligence,"* (Apr. 25, 2023), <https://www.consumerfinance.gov/about-us/newsroom/director-chopra-prepared-remarks-on-interagency-enforcement-policy-statement-artificial-intelligence/>.

¹³ FTC, *Statement of Chair Lina M. Khan Regarding the Presentation on Data Security At the December 2022 Open Commission Meeting*, at 1, (Dec. 14, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/12142022OCMKhanRemarksDataSecurityPresentation.pdf.

¹⁴ FTC, *FTC Releases 2023 Privacy and Data Security Update*, (Mar. 28, 2024), <https://www.ftc.gov/news-events/news/press-releases/2024/03/ftc-releases-2023-privacy-data-security-update>.

partial refunds to consumers.¹⁵ And in January 2024, the FTC charged X-Mode Social and its successor Outlogic with selling raw location data without obtaining informed consumer consent.¹⁶ The FTC alleged that these companies "sold precise location data that could be used to track people's visits to sensitive locations such as medical and reproductive health clinics, places of religious worship and domestic abuse shelters."¹⁷

The SEC is also increasing enforcement against data abuse and has recently prosecuted several offenders who failed to properly disclose the nature of their data breaches and protect consumer's sensitive information. For example, in March 2023, the SEC settled charges against a cloud-computing software for making misleading disclosures about a 2020 ransomware attack, which impacted over 13,000 customers for a civil penalty of \$3 million.¹⁸ Accordingly, companies should be forthright in their public disclosures about cybersecurity risks and attacks to avoid hefty fines and security investigations.

The DOJ has similarly expanded its technological capabilities on both the antitrust and data privacy fronts. For example, at the American Bar Association Antitrust Spring Meeting on April 12, 2024, Jonathan Kanter, United States Assistant Attorney General for the Antitrust Division, stated that the agency is investing in more technology to detect international cartels.¹⁹ Kanter discussed how this technology will prevent the agency from having to heavily depend on leniency applications. "Leniency is still a very important part of our program, but we are not solely relying on leniency as our source for case generation."²⁰

The DOJ has also increased use of AI to aid its white-collar criminal enforcement in technical industries. In February 2024, Deputy Attorney General Lisa Monaco announced a new effort – "Justice AI" – that will study the most efficient way for the DOJ to utilize and deploy AI technology to prosecute white-collar crime.²¹ In addition, the DOJ indicated that it would seek harsher sentences for violators who misuse disruptive technology to facilitate their offenses. Specifically, Monaco warned that "[w]here AI is deliberately misused to make a white-collar crime significantly more serious, our prosecutors will be seeking stiffer sentences – for individual and corporate defendants alike."²² Monaco further stated that prosecutors would assess how company compliance programs mitigate "the company's most significant risks . . . includ[ing] the risk of misusing AI."²³

To bolster DOJ's efforts at modernizing its enforcement capabilities to address abuses of emerging technologies, Attorney General Merrick Garland designated Jonathan Mayer as the DOJ's first Chief Science and Technology Advisor and Chief Artificial

¹⁵ FTC, *FTC Gives Final Approval to Order Banning BetterHelp from Sharing Sensitive Health Data for Advertising, Requiring It to Pay \$7.8 Million*, (July 14, 2023), <https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-gives-final-approval-order-banning-betterhelp-sharing-sensitive-health-data-advertising>.

¹⁶ FTC, *FTC Order Prohibits Data Broker X-Mode Social and Outlogic from Selling Sensitive Location Data*, (Jan. 9, 2024), <https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-prohibits-data-broker-x-mode-social-outlogic-selling-sensitive-location-data>.

¹⁷ *Id.*

¹⁸ SEC, *SEC Charges Software Company Blackbaud Inc. for Misleading Disclosures About Ransomware Attack That Impacted Charitable Donors*, (Mar. 9, 2023), <https://www.sec.gov/news/press-release/2023-48>.

¹⁹ Khushita Vasant, *US DOJ investing heavily in technology to detect international cartels*, MLex, (Apr. 12, 2024), https://content.mlex.com/#/content/1556049/us-doj-investing-heavily-in-technology-to-detect-international-cartels-kanter-says?referrer=search_linkclick.

²⁰ *Id.*

²¹ DOJ, *Deputy Attorney General Lisa O. Monaco Delivers Remarks at the University of Oxford on the Promise and Peril of AI*, (February 14, 2024), <https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-delivers-remarks-university-oxford-promise-and>.

²² DOJ, *Deputy Attorney General Lisa Monaco Delivers Keynote Remarks at the American Bar Association's 39th National Institute on White Collar Crime*, (Mar. 7, 2024), <https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-monaco-delivers-keynote-remarks-american-bar-associations>.

²³ *Id.*

Intelligence Officer.²⁴ Garland declared that the DOJ "must keep pace with rapidly evolving scientific and technological developments."²⁵ In this role Mayer will "spearhead the Department's technological capacity-building efforts, including by advising on recruiting technical talent to ensure the Department has the expertise and is equipped to meet the challenges ahead."²⁶

The improved technological capabilities and expertise of federal agencies including FCC, SEC, CFPB, FTC, and DOJ, as well as interagency coordination focused on targeting abuses of emerging technology and privacy and data violations will undoubtedly reshape the landscape of federal regulatory enforcement in these areas. Moving forward, these federal agencies will no longer view data concerns in isolation by sector, but instead collaborate to investigate privacy, communication, and competition issues. This interagency coordination will provide the agencies with even more tools and models to identify data misuse.

Takeaways

The increased use of technology and interagency coordination present new challenges for companies to consider.

Increased coordination allows the agencies to pool their resources, bring new cases, and take more aggressive enforcement actions. It also allows the federal agencies to take a more holistic and multi-faceted approach in investigating and challenging conduct. In these instances, agencies may seek to test new theories of harm and prosecute new cases with stronger execution. Companies that store and monetize data should expect to see increased scrutiny and enforcement across the board. Companies should also evaluate how responses provided in a given investigation can implicate compliance concerns in other regulatory areas.

Additionally, the sharing of new technologies and methodologies could change the way companies receive investigative inquiries. Agencies are increasingly employing technical models to identify potential violations. As a result, companies subject to investigation could receive inquiries that were generated through a proprietary AI or data analytics tool, which may pose novel questions about due process and discovery in these proceedings. Moving forward, responding to these enforcement actions may require technical experts to address these methods. Counsel should anticipate a whole host of issues arising from investigations brought about by technical models.

All in all, businesses should be mindful that increased coordination creates increased resources in pursuit of prosecutions. Agencies are leveling up their ability to investigate misconduct around data processing and AI and pursuing greater interagency coordination efforts. Companies should therefore look to increase coordination among their own regulatory teams and ensure their compliance programs are built in ways that consider that different regulatory concerns can arise with respect to the use of AI and handling of data.

²⁴ DOJ, *Attorney General Merrick B. Garland Designates Jonathan Mayer to Serve as the Justice Department's First Chief Science and Technology Advisor and Chief AI Officer*, (Feb. 22, 2024), <https://www.justice.gov/opa/pr/attorney-general-merrick-b-garland-designates-jonathan-mayer-serve-justice-departments-first>.

²⁵ *Id.*

²⁶ *Id.*

Contact Us



Peter Chan
Partner
Chicago
Washington, D.C.
peter.chan@bakermckenzie.com
[@bakermckenzie.com](https://twitter.com/bakermckenzie)



Elizabeth Roper
Partner
New York
elizabeth.ropер@bakermckenzie.com
[@bakermckenzie.com](https://twitter.com/bakermckenzie)



Mark Weiss
Partner
Washington, D.C.
mark.weiss@bakermckenzie.com
[@bakermckenzie.com](https://twitter.com/bakermckenzie)



Daniel Graulich
Associate
Washington, D.C.
daniel.graulich@bakermckenzie.com
[@bakermckenzie.com](https://twitter.com/bakermckenzie)



Allison Simkins
Associate
Washington, D.C.
allison.simkins@bakermckenzie.com
[@bakermckenzie.com](https://twitter.com/bakermckenzie)

© 2024 Baker & McKenzie. **Ownership:** This site (Site) is a proprietary resource owned exclusively by Baker McKenzie (meaning Baker & McKenzie International and its member firms, including Baker & McKenzie LLP). Use of this site does not of itself create a contractual relationship, nor any attorney/client relationship, between Baker McKenzie and any person. **Non-reliance and exclusion:** All information on this Site is of general comment and for informational purposes only and may not reflect the most current legal and regulatory developments. All summaries of the laws, regulation and practice are subject to change. The information on this Site is not offered as legal or any other advice on any particular matter, whether it be legal, procedural or otherwise. It is not intended to be a substitute for reference to (and compliance with) the detailed provisions of applicable laws, rules, regulations or forms. Legal advice should always be sought before taking any action or refraining from taking any action based on any information provided in this Site. Baker McKenzie, the editors and the contributing authors do not guarantee the accuracy of the contents and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the contents of this Site. **Attorney Advertising:** This Site may qualify as "Attorney Advertising" requiring notice in some jurisdictions. To the extent that this Site may qualify as Attorney Advertising, PRIOR RESULTS DO NOT GUARANTEE A SIMILAR OUTCOME. All rights reserved. The content of this Site is protected under international copyright conventions. Reproduction of the content of this Site without express written authorization is strictly prohibited.

