wiley

NEWSLETTER

Top Developments to Watch at the FTC on Privacy

June/July 2022

Privacy In Focus®

The Federal Trade Commission (FTC or Commission) now has a full slate of Commissioners with the confirmation and swearing-in of Commissioner Alvaro Bedoya, who brings an extensive background in privacy issues. The Commissioners have signaled that privacy and data security issues will be a priority for the FTC in the coming months and beyond, including: children's privacy, "commercial surveillance," artificial intelligence (AI), and data security practices. Below, we provide a summary of key developments in these areas.

Children's Privacy

On the children's privacy front, the FTC recently unanimously reaffirmed its support for active enforcement of children's online privacy protections. On May 19, 2022 in a 5-0 vote, the FTC adopted a Policy Statement directed to providers of education technology (Ed Tech) regarding their obligations under the Children's Online Privacy Protection Act (COPPA). The Policy Statement notes that the agency will focus COPPA enforcement actions on, among other things, violations of (1) prohibitions against mandatory data collection, (2) use prohibitions when schools have given consent to the collection (rather than the parent), (3) retention restrictions, and (4) security requirements.

Following the FTC's approval of the Policy Statement, staff attorneys published a blog post warning Ed Tech companies that "they must follow the law, including by properly safeguarding [children's] personal information and, where a company relies on the school to provide consent, using kids' information only for school-related

Authors

Duane C. Pozza
Partner
202.719.4533
dpozza@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Joan Stewart
Partner
202.719.7438
jstewart@wiley.law

Stephen J. Conley
Associate
202.719.4572
sconley@wiley.law

Tawanna D. Lee
Consulting Counsel
202.719.4574
tdlee@wiley.law

Practice Areas

FTC Regulation

Privacy, Cyber & Data Governance

purposes, not for things like marketing."

This activity comes amidst an increased focus on children's and teens' privacy from both federal and state policymakers, including recent COPPA-related enforcement actions by the FTC. Indeed, on a related note, the FTC will be holding a workshop in October also focused on kids and consumer protection – dealing with what it calls "stealth marketing" to children.

'*Commercial Surveillance' Rulemaking*

FTC Chair Lina Khan, in her April 2022 speech at the IAPP Global Privacy Summit, confirmed that the FTC was considering launching a rulemaking on practices it refers to as "commercial surveillance." As we have previewed, this rulemaking is likely to cover certain kinds of data collection and use, "lax security practices," and algorithmic decision-making. In particular, statements by the Chair and some FTC Commissioners in connection with recent enforcement actions reflect an ongoing concern with the large quantity of data collected about individuals and how it is used to create user profiles that allow a business or an ad network to deliver targeted advertising.

In her IAPP speech, Chair Khan acknowledged that at times, this collection of personal data can result in a customized service that is greatly appreciated by the consumer, but she expressed concerns about the "lack of legal limits" on what information can be monetized, and in particular that this business model "incentivizes endless tracking." She also argued that the FTC should approach data privacy protections not just in terms of "procedural" protections (such as privacy notice requirements) but also in terms of hard limits where certain practices are prohibited.

Notably, this skepticism of personal data collection and use for targeted advertising purposes is mirrored at the state level. All five state comprehensive privacy laws that take effect in 2023 will give consumers the right to opt out of targeted advertising – or in the case of California, the right to opt out of sharing for cross-context behavioral advertising. And three of the five laws include protections around using information collected about an individual for automated profiling.

The first public step in a "commercial surveillance" rulemaking will be release of an Advance Notice of Proposed Rulemaking, which will give further indication of the FTC's goals in this area.

Algorithms and AI

The FTC has been concerned about potential negative impacts of AI and algorithms – including the potential for bias – as we have previously discussed. On June 15, 2022, the FTC continued to expand on its criticism for AI, voting 4-1 (with Commissioner Phillips dissenting) to issue a Report to Congress, *Combatting Online Harms Through Innovation*. The Report highlights current uses of AI to combat specific online harms, including scams, fake reviews, deepfakes, dark patterns, hate crimes, harassment, and child sexual abuse. The Report's topline conclusion is that "governments, platforms, and others must exercise great caution in either mandating the use of, or over-relying on, [AI] even for the important purpose of reducing harms." Instead, the Report suggests that "any initial legislative focus should prioritize the transparency and accountability of platforms and others

that build and use automated systems to address online harms."

In supporting the Report to Congress, Chair Khan argued that many new AI technologies appear to be amplifying harmful and illegal content rather than curtailing it. Commissioners Slaughter and Bedoya were similarly supportive of the Report and discussed ways in which misuse of AI might cause greater harms. Commissioner Wilson also supported the Report, but noted that AI has the potential to generate both benefits and harms, and she cautioned that technology that swiftly labels controversial ideas as false could chill new ideas. On the other hand, Commissioner Phillips argued that the Report was too critical of AI, and it should have been based on a request for information from stakeholders.

The Report discusses a number of specific concerns with AI (e.g., potential bias, transparency, human oversight) that apply more generally, not just in terms of online harms. The FTC has signaled concerns with how AI is deployed in the past, and appears likely to continue its scrutiny via enforcement actions, reports, and potentially the "commercial surveillance" rulemaking discussed above.

Data Security

In addition to "lax security practices" being potentially covered in a new rulemaking, as noted above, the FTC continues to remain active on data security enforcement. For example, in the recent *CafePress* matter, the FTC alleged that the owners of the company CafePress failed to reasonably secure consumers' sensitive personal data, and its settlement will require the companies to pay $500,000 in addition to mandatory injunctive provisions.

In particular, the FTC's complaint alleged that CafePress, an online platform that allows consumers to purchase customized merchandise from other consumers or "shopkeepers," failed to "provide reasonable security for the Personal Information stored on its network." Among other things, CafePress allegedly failed to "implement readily-available protections, including many low-cost protections, against well-known and reasonably foreseeable vulnerabilities"; stored personal information on its network in clear text; and "created unnecessary risks" to personal information by storing it indefinitely on its network without a business need, which the FTC alleged to be a violation of the FTC Act. Also, the FTC alleged, in support of its claims, that the operators of CafePress failed to reasonably respond to security incidents, including by failing to "timely disclose security incidents to relevant parties, preventing them from taking readily available low-cost measures to avoid or mitigate reasonably foreseeable harm."

Indeed, one key takeaway of the CafePress action is that the FTC will scrutinize how companies respond when there is a data breach. The agency recently reaffirmed this in a May 20 Tech@FTC blog post on incident response and breach disclosure, going so far as to say that "in some instances, the FTC Act creates a de facto breach disclosure requirement because the failure to disclose will, for example, increase the likelihood that affected parties will suffer harm." Companies dealing with a breach will need to be prepared to assess whether their response will potentially raise issues under the FTC Act – an area in which the FTC has yet to provide clarity but may be more active.

***

With a full slate of Commissioners, we expect developments on these and other privacy and data security issues to continue in the coming months. Please reach out to the authors or anyone in Wiley's FTC Practice for further information.