BCLP. Client Intelligent

Insights

FTC CYBERSECURITY AND DATA PRIVACY ROUNDUP

May 14, 2024

SUMMARY

Last year was a pivotal one for data privacy, as privacy received substantial attention from many regulators, including the Federal Trade Commission ("FTC"). Looking back at the FTC's 2023 enforcement actions, statements and policies provides attorneys and clients with a helpful compliance roadmap of what is to come.

ENFORCEMENT ACTIONS

2023 brought a wave of FTC enforcement actions largely focused on online tracking technologies, children's privacy, the reasonableness of privacy and cybersecurity practices, and geolocation data that carried hefty fines and various penalties for companies across a variety of industries.

ONLINE TRACKING TECHNOLOGIES – COMPARING PROMISES TO ACTIONS

One clear area of focus was protecting digital health by regulating online tracking technologies. The FTC brought multiple actions, including under the Health Breach Notification Rule[1]("HBNR"), alleging that digital health platforms GoodRx, Betterhelp, and Premom collected and improperly shared consumers' sensitive health information with third parties and monetized that health data for targeting advertising in violation of the FTC Act[2], the HBNR, and the entity's own privacy policies. Specifically, the FTC advanced the theory that sharing data with third parties was an unauthorized disclosure of individually identifiable health information and constituted a breach of security under the HBNR.[3] These actions resulted in significant monetary penalties of $1.5 million (GoodRx), $7.8 million (Betterhelp), and $100,000 (Premom), and a variety of non-monetary penalties including prohibitions on data sharing, limitations on data retention, and new mandates for privacy policies and programs. They provide a clear warning to non-HIPAA covered businesses in the healthcare space.

And the FTC recently finalizing changes to the HBNR that clarify its applicability to health apps and similar technologies, so this trend is likely to continue. Businesses should take a close look at the

tracking technologies used on their websites and apps and ensure their practices line up with their privacy disclosures, focusing in particular on what data is disclosed, to whom, and the limitations imposed on third-party recipients' use of that information.

CHILDREN'S PRIVACY – DARK PATTERNS, COLLECTION, AND COMMUNICATION

Another area of focus has been technology and software companies whose platforms target, and are accessed by, children for violations of the Children's Online Privacy Protection Rule[4]("COPPA") and the FTC Act. Amazon was fined $35 million for allegedly indefinitely retaining written transcripts of children's voice recordings through the Amazon Alexa product and misleading parents about their ability to delete their child's voice recording. Additionally, the FTC modified its 2020 order to fine Meta $5 billion for allegedly allowing children to communicate with contacts who were not approved by their parents on its Messenger Kids product and allowing app developers access to children's private data. Microsoft also received a $20 million fine for allegedly failing to obtain parental consent before its Xbox product collected and retaining children's personal information for longer than was reasonably necessary. In this action, the FTC extended COPPA protections to third-party gaming publishers with whom data is shared, and clarified that avatars generated from a child's image are covered by COPPA when collected with other personal information (e.g., information that would reveal that the avatar relates to a child's account). Lastly, Edmodo, a company that creates education technology tools, received a $6 million fine for allegedly failing to obtain verifiable parental consent before collecting children's data, using children's personal information for advertising, and allegedly unlawfully outsourcing its COPPA compliance responsibilities to schools.

These actions demonstrate the FTC's commitment to protecting children's online privacy and regulating how children's data is collected and used. Organizations that collect children's data must ensure they obtain parental consent in compliance with COPPA, only collect information as is reasonably necessary, and store data for only a reasonable amount of time. They should also evaluate statements on their privacy policies and confirm that their internal policies match the commitments therein.

REASONABLE PRIVACY AND CYBERSECURITY PRACTICES

Another area of focus has been violations of Section 5 of the FTC Act[5]for privacy and cybersecurity practices. Although they did not receive monetary penalties, actions were brought against Drizly and Chegg for allegedly inadequate practices, which included misrepresentations and deceptive statements. The FTC categorized their practices as "careless" and alleged that statements in their privacy policies claiming they implemented reasonable security measures were deceptive.

In its action against Ring, the FTC claimed that Ring's lax security measures and allowance of overly permissive access exposed sensitive consumer data to exploitation by hackers. Ring was

also penalized for failing to adequately notify or obtain consumer consent for its extensive human review of private video recordings to train its algorithms. Specifically, the FTC determined that general statements in privacy policies and terms of use that permit companies to use consumer data for product improvement and development are insufficient to justify using that content to train algorithms or for other artificial intelligence purposes if the data is reviewed by humans. This renews focus on privacy disclosures at a time when many companies are investigating the feasibility of AI applications.

In a unique action against 1Health.io, the FTC claimed that 1Health.io misled consumers about its data sharing practices with third parties by retroactively changing its policy without properly notifying and obtaining consent from consumers. This action makes clear that when making material retroactive changes to privacy policies, the FTC may require companies to notify consumers of those changes.

GEOLOCATION DATA

Although the FTC filed a sealed complaint against data broker Kochava in 2022, its 2023 unsealed amended complaint provides insight on the FTC's expectations for the collection of geolocation data. The complaint demonstrates the FTC's concerns about the collection and sharing of geolocation data and alleges that by selling the geolocation tracking data collected from hundreds of millions of mobile devices, Kochava enabled third parties to trace identified individuals' movements to and from sensitive locations, thereby exposing them to threats of stigma, stalking, discrimination, job loss, and potential physical violence.

Implications for 2024: This pending action is set to move full steam ahead in 2024, with the District Court of Idaho denying Kochava's motion to dismiss on February 5th, 2024. Businesses that collect geolocation data should follow this case carefully, as its result will likely have important implications for the collection and sharing of geolocation data.

STATEMENTS AND POLICY POSITIONS

In addition to enforcement actions, the FTC also made its position on many privacy issues clear through a number of statements and policy positions in 2023.

In May, the FTC issued a Biometrics Warning that expressed concern about the increased use of consumer biometric information and related technologies powered by machine learning. Specifically, it stated that the use of these technologies raises significant consumer privacy and data security concerns and the potential for bias and discrimination. The FTC asserted that it will combat unfair or deceptive acts and practices related to the collection and use of consumer biometric information and the use of biometric information technologies. In this Warning, the FTC listed factors it will use to determine whether a businesses' use of these technologies constitute unfair or deceptive practices in violation of the FTC Act. Organizations can use these factors, which

include addressing known or foreseeable risks and providing appropriate training, as a roadmap for compliance policies and procedures if it collects and uses biometric data.

In addition to the Warning, the FTC made additional statements addressing its concerns about discrimination and bias in automated systems. In a joint statement, the FTC and other regulatory agencies resolved to vigorously use their collective authorities to combat discrimination and bias and monitor the development and use of automated systems to promote responsible innovation. The FTC also published a resolution in November that purports to grant it the ability to more easily issue civil investigative demands in non-public investigations into AI-related products and services.

The FTC followed through on some of these concerns in a July 2023 action against ChatGPT. In that investigation, the FTC demanded ChatGPT's records on how it addresses risks related to AI models to investigate if it has engaged in unfair or deceptive privacy or data security practices, or has engaged in unfair or deceptive practices related to risk of harm to consumers. Additionally, the FTC announced its settlement with Rite Aid late in 2023, which alleges that Rite Aid deployed AI recognition technology without reasonable safeguards that falsely tagged consumers as shoplifters, particularly women and people of color.

CONCLUSION

The FTC is concentrating on preventing unfairness and bias that could be passed down to consumers through technological innovations. We are likely to see this focus continue to expand through enforcement actions that should give organizations the opportunity to consider how to use technological innovations while protecting consumer data. In particular, companies utilizing artificial intelligence and machine learning algorithms, and those processing health data and geolocation data, should brace for an increase in scrutiny and further FTC guidance.

FOOTNOTES

[1] 16 CFR Part 318.

[2] 15 U.S.C. §§ 41-58.

[3] The FTC's 2021 Policy Statement provided guidance on the scope of the HBNR, which included its coverage of most health apps not covered under HIPAA, and explained that a breach of security may occur as a result of an organizations own actions, and is not limited to cybersecurity intrusions or nefarious behavior. The 2023 actions were the first actions the FTC took under the HBNR and the first to demonstrate the 2021 policy statement.

[4] 16 CFR Part 312.

[5] 15 U.S.C. § 45(a).

RELATED PRACTICE AREAS

- Data Privacy & Security

MEET THE TEAM

Amy de La Lama

Boulder

amy.delalama@bclplaw.com
+1 303 417 8535

Christian M. Auty

Chicago

christian.auty@bclplaw.com
+1 312 602 5144

Annalisa Kolb

Chicago

annalisa.kolb@bclplaw.com
+1 312 602 5062