

Federal Trade Commission Looking at New Rules to Combat Discrimination in Algorithms and Poor Security Practices

JANUARY 20, 2022

Authors: [Ryan T. Sulkin](#)

The brief FTC note indicates the agency will look to combat poor security practices, protect against the misuse of personal information, and discrimination arising from algorithmic decision-making. Last month, the Federal Trade Commission (“**FTC**”) submitted a brief summary of potential rules it may look at implementing over the course of 2022 to the Office of Management and Budget (“**OMB**”). The summary comes on the heels of a letter from FTC Commissioner Lina Khan to Sen. Richard Blumenthal, who is the chair of the Committee on Commerce, Science, and Transportation; as well as the chair of the subcommittee on Consumer Protection, Product Safety, and Data Security.

According to Commissioner Khan, any such rulemaking would be conducted under an [updated, streamlined](#) rule making process. The updated process eliminates time consuming elements of the rulemaking process (such as staff reports and analysis) that are not specifically required by law. The hope is that the streamlined process will allow for rules and regulations to be timelier, instead of one or two steps behind the technology it regulates.

While no draft or final rule is published yet, the summary and letter show an increased interest in more privacy and data protection regulation from the FTC.

Congress [has been calling](#) on the federal government to implement new rules and regulations on such matters, and the letter specifically addresses such calls. Congress has also proposed a litany of new laws; some geared at tech anti-trust, some geared at omnibus privacy protection. However, no legislation is close to being taken up for serious consideration.

Possible New Privacy Regulation

The summary and letter highlight three specific areas where the FTC will look into adopting new regulations: (1) security practices; (2) protection against the misuse of personal information; and (3) protection against discrimination that may arise from algorithmic decision-making.

First, the FTC may take new action against poor security practices. This is in line with other FTC and federal government action, which has recently heightened its focus on specific security measures that business must adopt in order to guard against the rising threat that cybersecurity incidents pose to individuals and the U.S. For example, the FTC recently issued an [amended Safeguards rule](#) requiring financial institutions to implement specific security measures (such as multi-factor authentication and encryption).

Future FTC rulemaking in this area may broadly apply specific security standards to a broader swath of businesses, in order to combat lax security standards.

Second, in order to protect consumers from the misuse or abuse of their personal information, the FTC may consider new rules on so called “dark patterns.” Dark patterns are ploys that businesses use to mislead consumers into purchasing certain goods or services, or use to get consumers to agree to certain contracts, terms, or agreements. Any deceptive practice that is built into a business’s user-interface that-intentionally or unintentionally-obscures or subverts a consumer’s independent choices, is considered a dark pattern. It can also include instances where a business misleads a consumer into giving their personal information away.

For example, if a business’s systems interpret a lack of a choice, or silence, as consent, such a practice could be considered a dark pattern. According to Commissioner Khan, any FTC regulation on dark patterns would address the “serious shortcomings” of the current notice-and-choice privacy approach that U.S. law is largely based on.

Third, the FTC will look into rules and regulations to protect consumers from discrimination in algorithmic decision-making. Algorithms are traditionally protected by intellectual property laws because they are normally considered trade secrets. Therefore, algorithms do not face thorough, independent vetting.

Here, the FTC could consider rules that protect groups of consumers from being “disfavored” by the algorithms based on an individual’s protect status, including religion, race, medical status, gender, or sexual orientation. Businesses could be required to properly review their algorithms and implement policies and procedures to ensure algorithms are developed in a way that guards against intentional or unintentional discrimination.

Moving Forward

On both sides of the aisle and across all branches, the federal government is increasing their focus on privacy and data protection. As new rules and regulations are proposed and adopted, businesses will need to stay on top of evolving, and likely more onerous, privacy and cybersecurity standards.

As federal agencies and regulators continue to adopt new privacy rules and amend already existing privacy rules, the Benesch Data Protection and Privacy team is committed to staying at the forefront of knowledge and experience to assist our clients in compliance efforts. We are available to assist you with any compliance needs.

Ryan T. Sulkin at rsulkin@beneschlaw.com or 312.624.6398.

Lucas Schaetzel at lschaetzel@beneschlaw.com or 312.212.4977.