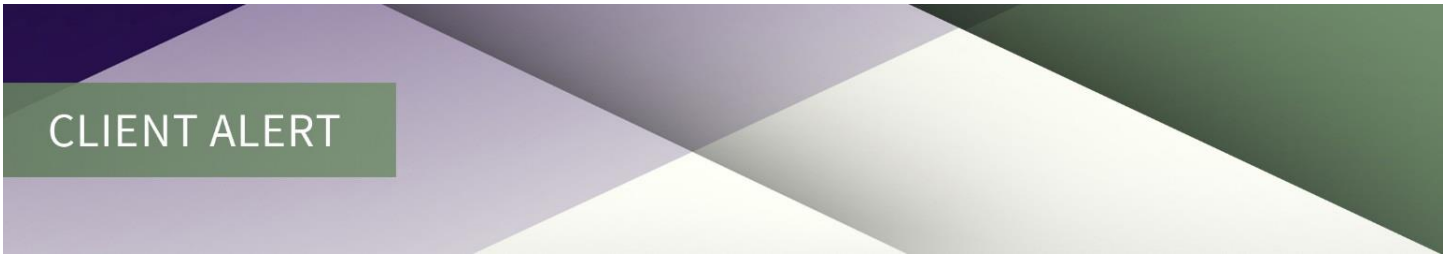

Federal Trade Commission Exploring Expanded Remedial Authority for Privacy and Data Security Matters

August 13, 2018

AUTHORS

Daniel K. Alvarez | Elizabeth J. Bower | Philip F. DiSanto | Jill Guidera Brown

Introduction

In response to evolving business practices, new technologies, and international developments, the Federal Trade Commission ("FTC" or "Commission") is considering whether it, too, might need to modernize. The Commission published a Notice on August 8, 2018, announcing that it will hold several hearings in the coming year as part of its "Competition and Consumer Protection in the 21st Century" program to collect input from stakeholders and thought leaders on emerging issues affecting the FTC's enforcement and policy agenda. The FTC is collecting public comment for this stage of the process through August 20, 2018. Among the many topics about which the FTC is soliciting input, the key privacy and security issues are: (1) the FTC's remedial authority to deter unfair and deceptive conduct in privacy and data security matters; (2) the consumer welfare implications associated with the use of algorithmic decision-making tools, artificial intelligence, and predictive analytics; and (3) the intersection between privacy, big data, and competition. The FTC invites general commentary on these topics, as well as insights from specific industries, such as healthcare, technology, and energy.

Background

Given recent developments in the U.S. and international privacy and data security landscape, it is no surprise that privacy and data security issues feature heavily in the FTC's "21st Century" program. On the global stage, the European Union

(EU)'s General Data Protection Directive (GDPR), which came into effect on May 25, 2018, requires companies that process the data of EU data subjects to adopt extensive technical and organizational measures, as well as to adhere to specified data security systems. Stateside, the hastily enacted California Consumer Privacy Act (CCPA) echoes many of the consumer transparency and control requirements of the GDPR, yet distinguishes itself from the EU law by prohibiting companies from discriminating against consumers that choose to opt out of data disclosures and by providing for a private right of action. A bill similar to the CCPA was recently proposed in the New Jersey Assembly, and other states may follow suit.

U.S. state legislatures are increasingly adopting data privacy laws that require careful attention from companies that operate websites or provide online goods or services nationwide. For example, Vermont's data broker bill includes new breach notification procedures and imposes a duty on data brokers to adopt a security program that protects personal information, and Illinois's Biometric Information Privacy Act requires companies to provide written notice and obtain consent prior to collecting biometric identifiers and to publish data retention schedules.

Federal privacy law currently consists primarily of sector-specific laws designed to protect certain categories of sensitive information (*e.g.*, children's data, health records, and driver's license information), with the FTC's authority to prohibit "unfair and deceptive practices" providing more general protection. However, the Trump Administration and the Commerce Department are currently meeting with stakeholders to develop a potential framework for the nation's first overarching federal privacy law. While such efforts have not yet crystallized into a legislative proposal, any proposal would likely regulate the way companies collect, use, and secure U.S. consumers' personal information, and may preempt state efforts like the CCPA.

Against this backdrop, the FTC's request for public comment is timely, given the need to define the Commission's role in providing policy guidance and bringing enforcement actions.

Expanded Remedial Authority for Privacy and Data Security Matters

With respect to its remedial authority to deter unfair and deceptive conduct in privacy and data security matters, the Commission is soliciting public comments on (i) the efficacy of the Commission's use of its current remedial authority and (ii) the identification of any additional tools or authorities the Commission may need to adequately deter unfair and deceptive conduct related to privacy and data security. The FTC's consideration of its remedial authority comes on the heels of the Eleventh Circuit's decision in *LabMD v. FTC*, No. 16-16270 (11th Cir. June 6, 2018), in which the Eleventh Circuit found that an FTC cease-and-desist order issued against a company for failing to implement "reasonable" security measures was unenforceable because the order was too vague and did not describe an actual unfair act or practice.

In response to the *LabMD* decision, commentators have debated whether the FTC's "reasonable" standard is sufficient to encompass the complex technical and organizational security measures required by modern cybersecurity practices.

While some have argued that the FTC may need authority to adopt standards that provide more tailored guidance for companies that collect and maintain consumer data, others have argued that the FTC's current approach is sufficient, and granting the FTC further authority is likely to overly restrict industry innovation.

Consumer Welfare Implications of Algorithmic Decision Tools, Artificial Intelligence, and Predictive Analytics

Companies across industries increasingly rely on cutting-edge technologies such as machine learning, predictive analytics, artificial intelligence, and autonomous and connected vehicles. With these technologies come novel ethical and privacy issues. As such, the FTC requests public comment on (i) the welfare effects and privacy implications associated with the use of these tools; (ii) the welfare implications associated with the use of these technologies in the determination of a firm's pricing and output decisions; and (iii) whether restrictions on the use of computer and machine learning and data analytics affect innovation or consumer rights in existing or future markets. An assessment of consumer welfare in this context will likely require stakeholders to consider the benefits consumers derive from these technologies, as well as potential risks that the use of these technologies present to individual consumers and to the market.

In December 2017, the New York City Council passed an "algorithmic accountability" bill that establishes a task force to develop processes for greater transparency in how automated decisions are made and to assess instances of bias or discrimination in New York City's automated decision-making practices. The FTC may similarly focus on transparency and accountability, particularly with respect to how consumers are notified that their data is used in algorithmic decision-making, and how the results of those automated processes are presented to consumers.

Intersection Between Privacy, Big Data, and Competition

The Notice also seeks public comment on the intersection of privacy, big data, and competition, and reflects the Commission's interest in exploring (i) control of data as a dimension of competition; (ii) competition on privacy and data security attributes (*e.g.*, the comparative security of social media platforms or messaging products); (iii) consumer preferences with respect to business models driven by the collection and use of big data; (iv) the costs and benefits of varying (and sometimes conflicting) state, federal and international privacy laws and regulations; and (v) the competition and consumer protection implications of "use and location tracking mechanisms." The Commission has discussed these topics in prior reports on the "Internet of Things" and Big Data, but significant developments in the technological and legal landscapes make their continued exploration timely.

The Commission is not alone in exploring the competitive and consumer protection implications of "big data." The Deputy Assistant Attorney General of the Antitrust Division of the Department of Justice, for example, commented recently that forcing competitors to share access to data "is just as (or perhaps more) likely to result in less . . . innovation as it is to enable new competition within existing markets." European regulators and enforcement agencies have also focused specifically on the collection, aggregation, and use of consumer data to engage in anticompetitive conduct. For example,

the German Federal Cartel Office ("FCO") has taken the position that a company may violate data protection and competition laws by improperly collecting and merging data from third parties to abuse its dominance in a particular market. The FTC is likely to remain interested in similar issues regarding its dual mandate of promoting competition and protecting consumers.

***

The FTC will seek public comment in stages throughout this initiative, with the current stage remaining open until August 20, 2018. Hearings are anticipated to take place from September 2018 through January 2019 in locations throughout Washington, D.C. and elsewhere in the country. Comments can be submitted via the FTC's website or by mail, but note that comments may be made publically available on the Commission's website. The FTC anticipates that its staff and leadership will use the comment and hearing process as an opportunity to think critically about the Commission's policy agenda and enforcement mechanisms, and update them as needed to better reflect business and technological practices in the 21st century.

If you have any questions regarding this client alert, please contact the following attorney or the attorney with whom you regularly work.

Daniel K. Alvarez
202 303 1125
dalvarez@willkie.com

Elizabeth J. Bower
202 303 1252
ebower@willkie.com

Philip F. DiSanto
212 728 8534
pdisanto@willkie.com

Jill Guidera Brown
202 303 1217
jgbrown@willkie.com