August 2022

Skadden

Privacy & Cybersecurity Update

FTC Announces Advance Notice of Proposed Rulemaking Regarding Data Privacy and Data Security

On August 11, 2022, the Federal Trade Commission (FTC) released an advance notice of proposed rulemaking (ANPR), seeking public comment on the topics of data privacy and cybersecurity. This comes at a significant moment in the context of privacy regulation in the U.S., as an increasing number of states adopt their own privacy laws and Congress considers whether to move forward with the draft American Data Privacy and Protection Act (ADPPA).[1] With the ANPR, the FTC aims to pressure Congress to move forward with the adoption of a national data privacy law such as the ADPPA, while at the same time adopting new rules that will provide businesses with clearer guidance regarding the use and protection of personal data in the event that Congress fails to act.

Background

FTC Chair Lina Khan has made increasing the protection of personal data and individuals' privacy in the United States a significant part of her focus since she was appointed in June 2021. However, until recently, the FTC had made little progress in this regard, as the Commission was experiencing a 2-2 deadlock along party lines amongst its commissioners. With the confirmation of Commissioner Alvaro Bedoya in May 2022, the deadlock has been broken and the FTC will now be able to move forward with its proposed rulemaking process.

Using its specific authority under the Gramm-Leach-Bliley Act (among other laws) and its general authority under the FTC Act to prohibit "unfair or deceptive acts or practices in or affecting commerce," the FTC has been the primary regulator of privacy and data security practices in the U.S. for decades. Over the past few years, the FTC has faced setbacks as a result of various court decisions that invalidated or curtailed the FTC's enforcement and rulemaking authority. For many privacy advocates, the ANPR is a welcome initiative to protect consumer privacy and create clearer requirements for businesses to follow.

[1] See our June 2022 *Privacy & Cybersecurity Update* article "Bipartisan Congressional Group Proposes Comprehensive Federal Privacy Law."

The Process and Scope of the ANPR Filing

The ANPR Process

The first step in the FTC rulemaking process is for the Commission to publish an ANPR, thereby requesting public comment. In this August filing, the ANPR is focused on "the prevalence of commercial surveillance and data security practices that harm consumers." Specifically, the FTC posed 95 questions and invited comment on whether it should implement new regulations regarding how companies "(1) collect, aggregate, protect, use, analyze, and retain consumer data, as well as (2) transfer, share, sell, or otherwise monetize that data in ways that are unfair or deceptive." The comments must be received on or before 60 days after the date of publication in the federal register. In addition, a public forum is scheduled to be held virtually on September 8, 2022, to discuss these topics.

After receiving comments in connection with the ANPR, if the FTC decides to proceed with a proposed rulemaking, certain congressional committees must receive notice 30 days before the notice of proposed rulemaking is published. The next steps would then include the FTC publishing a notice of proposed rulemaking, followed by informal hearings and the development of the final rule. Due to the uncertainty of the public commentary, as well the possibility of the ADPPA or another federal privacy law being passed and the lengthy process of rulemaking, the future for such new rule (if any) is uncertain.

The Scope of the ANPR

As noted above, the scope of the August 2022 ANPR is quite broad, including a multitude of privacy and data security issues on such topics as artificial intelligence, biometrics, targeted advertising and the protection of employees. The ANPR adopts broad definitions for various terms, further highlighting the breadth of the FTC's considerations. Notably, the term "consumer" includes "businesses and workers, not just individuals who buy or exchange data for retail goods and services." Similarly broad in scope, "data security" refers to "breach risk mitigation, data management and retention, data minimization, and breach notification and disclosure practices." Additionally, the ANPR defines "commercial surveillance" as "the collection, aggregation, analysis, retention, transfer, or monetization of consumer data and the direct derivatives of that information."

In addition to the aforementioned 95 questions, the FTC invites public comment regarding "(a) the nature and prevalence of harmful commercial surveillance and lax data security practices, (b) the balance of costs and countervailing benefits of any given potential trade regulation rule, and (c) proposals for protecting consumers from harmful and prevalent commercial surveillance and lax data security practices."

The Goals of the ANPR

The primary stated goal of the FTC's ANPR is to protect consumers from significant harms arising from "harmful commercial surveillance and lax data security." Chair Khan noted in a statement regarding the ANPR that "the growing digitization of our economy—coupled with business models that can incentivize endless hoovering up of sensitive user data and a vast expansion of how this data is used—means that potentially unlawful practices may be prevalent. Our goal today is to begin building a robust public record to inform whether the FTC should issue rules to address commercial surveillance and data security practices and what those rules should potentially look like." Through this process, the FTC hopes to provide clarity and predictability to businesses regarding the law's "application to existing and emergent commercial surveillance and data security practices." The expectation is that these new rules will do more to prevent and mitigate harms from uses of consumer data, as "enforcement alone without rulemaking may be insufficient to protect consumers from significant harms" — in part, because the FTC lacks the authority to seek civil penalties for first-time violators.

Secondarily, the ANPR serves an information-gathering tool for the Commission. The FTC's press release regarding the ANPR notes that "while very little is known about the automated systems that analyze data companies collect, research suggests that these algorithms are prone to errors, bias, and inaccuracy. As a result, commercial surveillance practices may discriminate against consumers based on legally protected characteristics like race, gender, religion, and age, harming their ability to obtain housing, credit, employment, or other critical needs." In sum, the FTC recognizes that to prevent substantial harms resulting from the use of consumer data, it is necessary to understand the nature, scope and prevalence of such harms.

Finally, FTC commissioners have been transparent in stating that the ANPR also is being used as a pressure mechanism, with the aim of galvanizing Congress to adopt a federal privacy law to address these issues. All five commissioners stated in their respective opinions that they would prefer Congress pass the ADPPA instead of having the FTC engage in this rulemaking process. Additionally, the ANPR itself notes that it is aimed at generating a public record about these practices, and that the comments will refine the FTC's work and inform reform by Congress and other policymakers "even if the FTC does not ultimately promulgate new trade regulation rules."

Key Takeaways

The filing of the ANPR marks a more proactive shift to the FTC's approach to privacy regulation. If the rulemaking process ultimately results in new privacy and cybersecurity regulations, this could dramatically affect the U.S. regulatory landscape for both consumers and businesses — including stricter rules and greater enforcement, combined with added clarity and predictability. However, the outcome of the rulemaking process is uncertain and will likely be largely dependent upon progress by Congress, or lack thereof, in adopting a new federal privacy law in the near future.

Return to Table of Contents

European Data Protection Board Issues Draft Guidelines on Calculation of Administrative Fines Under the GDPR

Earlier in 2022, the European Data Protection Board (EDPB) published draft guidelines on the calculation of administrative fines under the GDPR, aiming to bring greater harmony to the level of administrative fines set by supervisory authorities.[2]

Background

Article 83 of the GDPR provides that a supervisory authority has discretion to calculate the amount of an administrative fine, following a case-by-case evaluation and always subject to the rules of the GDPR. Such rules include, among others, that the fine amount must be tailored, in each case, to be effective, proportionate and dissuasive; that the supervisory authority take into consideration the severity of the relevant infringement and the conduct of the perpetrator; and that the amount of the administrative fine set not exceed the maximum amounts prescribed in Articles 83(4)-(6) of the GDPR following an evaluation of the circumstances of the case.

The guidelines, which supplement existing guidance[3] on the circumstances in which a supervisory authority should impose an administrative fine, aim to help standardize the methods supervisory authorities across Member States use to calculate such a fine by setting forth a five-step method to determining fines. Each such step is described below.

Step 1: Identify the Relevant Processing Operations and Evaluate Applicability of Article 83(3) of the GDPR

The analysis begins with the supervisory authority considering the relevant conduct and infringements to identify where fines may be issued. A single instance of conduct could give rise to a single infringement, or to multiple infringements, and the EDPB notes that, at times, "the same or linked processing operations" may constitute a single instance of conduct. The guidance provides examples of processing operations that are considered so interrelated that they can be considered as forming the same instance of conduct.

Where the perpetrator's behaviors give rise to a single infringement, the supervisory authority may calculate the fine on the basis of such infringement and its legal maximum. However, where multiple infringements arise out of the same sanctionable conduct, the supervisory authority must determine whether one infringement is a superseding infringement (*i.e.*, precludes or subsumes the applicability of the other infringements[4]) or whether the fine is calculated based on all applicable infringements arising from the sanctionable conduct (in which case, the legal maximum shall not exceed the amount specified for the most serious infringement). Where, instead, multiple sanctionable instances of conducts take place, the offenses are to be handled and fined separately.

Step 2: Determine a Starting Point To Calculate the Fine

A supervisory authority should begin their determination of the fine by assessing the following three elements to arrive at a starting point:

1. The classification of the infringement under Articles 83(4)-(6) of the GDPR, which determine whether the infringement falls into lower or higher fine tiers.
2. The nature, gravity and duration of the infringement, while also considering the scope and processing conduct at issue, the number of relevant data subjects affected, the degree of damages suffered and the character of the perpetrator (*i.e.*, negligent or intentional) to classify the severity of the infringement and set a starting fine. Where the severity level is determined to be low, the calculation is set to a small percentage (0-10%) of the legal maximum; where the severity level is determined to be high, the calculation is set to a higher percentage (20-100%).
3. The global annual turnover applicable to the undertaking (which relates not only to the relevant processor or controller legal entity that causes the breach, but to the wider group that it is part of). The figures generated in this step constitute the starting points for additional calculation.

[2] The draft guidelines on the calculation of administrative fines under the GDPR are available here.

[3] The guidelines on the application and setting of administrative fines for the purpose of the Regulation 2016/678 (*i.e.*, the GDPR) (WP253), adopted by the Article 29 Working Party (the predecessor to the EDPB), are available here.

[4] The application of one provision may preclude or subsume the applicability of another based on the principles of specialty (*e.g.*, a specific provision supersedes a general provision), subsidiary (*i.e.*, one infringement is considered subsidiary to another) or consumption (*i.e.*, one infringement regularly leads to the infringement of another). Where this occurs, the amount of the fine should be calculated based on the superseding infringement.

Step 3: Determine Whether Aggravating or Mitigating Circumstances Apply

Once a supervisory authority reaches a baseline to calculate a fine, it must analyze the specific circumstances of the infringement to determine whether the fine should be adjusted accordingly. Article 83(2) of the GDPR includes numerous aggravating and mitigating considerations, including: (1) the perpetrator's actions to mitigate damages to data subjects; (2) whether the perpetrator behaved in the manner expected in consideration of the infringement; (3) whether the perpetrator has committed infringements in the past; (4) how such perpetrator behaved following such infringements; (5) how and from whom the supervisory authority learned of the infringement; (6) whether the infringement is a repeat or similar version of past infringing behavior by the same perpetrator; and (7) other considerations, such as any direct or indirect financial profit received as a result of the infringement.

The EDPB notes that not all circumstances, even if positive, can constitute mitigating factors. For example, findings that a perpetrator had no past infringements or that the perpetrator behaved as it should with the supervisory authority may be neutral factors but will generally not mitigate a fine.

Step 4: Identify the Maximum Fine That Can Be Issued

The determination of a maximum penalty is dependent on whether the infringement is classified in Step 2 as falling into the higher or lower fee tiers. The maximum fine amount under Articles 83(4)-(6) of the GDPR will be the greater sum between a fixed amount (€10 million for the lower tier and up to €20 million for the higher tier), or a percentage (2% or 4%, respectively) of the annual global turnover of the undertaking.

Step 5: Determine Whether the Calculated Final Amount Meets the GDPR's Requirements

The GDPR requires that a fine be (1) effective (that it achieve the goals it intended to achieve); (2) dissuasive (that it have a deterrent effect both publicly and privately); and (3) proportionate (that the fine imposed reflects both the severity of the infringement and the size of the undertaking to which the perpetrator belongs, but that the fine also not go beyond what is necessary to be effective). After determining the level of the fine in steps 1 through 4, such fine should then be adjusted as necessary to account for these requirements (within the prescribed maximums determined in Step 4).

Key Takeaways

Though the introduction of the five-step methodology for calculating administrative fines brings consistency to the approach supervisory authorities should take when calculating fines for infringements of the GDPR, there is no guarantee that it will result in the harmonization of the fines themselves. The guidelines emphasize the fact that this methodology does not create a "precise mathematical calculation" for administrative fines and leave supervisory authorities with wide discretion in evaluating the factors that determine the final amount.

The guidelines were subject to a public consultation through June 27, 2022. A final version will be adopted in the period following the consultation, taking into account public comments.

Return to Table of Contents

Contacts

Stuart D. Levi
Partner / New York
212.735.2750
stuart.levi@skadden.com

James Carroll
Partner / Boston
617.573.4801
james.carroll@skadden.com

Brian Duwe
Partner / Chicago
312.407.0816
brian.duwe@skadden.com

David Eisman
Partner / Los Angeles
213.687.5010
david.eisman@skadden.com

Patrick Fitzgerald
Partner / Chicago
312.407.0508
patrick.fitzgerald@skadden.com

Todd E. Freed
Partner / New York
212.735.3714
todd.freed@skadden.com

Marc S. Gerber
Partner / Washington, D.C.
202.371.7233
marc.gerber@skadden.com

Rich Grossman
Partner / New York
212.735.2116
richard.grossman@skadden.com

Ken D. Kumayama
Partner / Palo Alto
650.470.4553
ken.kumayama@skadden.com

Michael E. Leiter
Partner / Washington, D.C.
202.371.7540
michael.leiter@skadden.com

William Ridgway
Partner / Chicago
312.407.0449
william.ridgway@skadden.com

Jason D. Russell
Partner / Los Angeles
213.687.5328
jason.russell@skadden.com

David Schwartz
Partner / New York
212.735.2473
david.schwartz@skadden.com

Ingrid Vandenborre
Partner / Brussels
32.2.639.0336
ingrid.vandenborre@skadden.com

Helena Derbyshire
Of Counsel / London
44.20.7519.7086
helena.derbyshire@skadden.com

Peter Luneau
Counsel / New York
212.735.2917
peter.luneau@skadden.com

James S. Talbot
Counsel / New York
212.735.4133
james.talbot@skadden.com

Eve-Christie Vermynck
Counsel / London
44.20.7519.7097
eve-christie.vermynck@skadden.com

This communication is provided by Skadden, Arps, Slate, Meagher & Flom LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This communication is considered advertising under applicable state laws.

Skadden, Arps, Slate, Meagher & Flom LLP
One Manhattan West
New York, NY 10001
212.735.3000