

Analysis of Proposed Consent Order to Aid Public Comment
In the Matter of NTT Global Data Centers Americas, Inc.
as successor in interest to RagingWire Data Centers, Inc.
Docket No. 9386; File No. 1823189

The Federal Trade Commission (“Commission”) has accepted, subject to final approval, an agreement containing a consent order from NTT Global Data Centers Americas, Inc., formerly known as RagingWire Data Centers, Inc. (“NTT Global”). The proposed consent order seeks to resolve allegations against NTT Global in the administrative complaint issued by the Commission on November 7, 2019.

The proposed consent order (“proposed order”) has been placed on the public record for thirty (30) days for receipt of comments by interested persons. Comments received during this period will become part of the public record. After thirty (30) days, the Commission will again review the agreement and the comments received, and will decide whether it should withdraw from the agreement and take appropriate action or make final the agreement’s proposed order.

This matter concerns alleged false or misleading representations by NTT Global concerning its participation in, and compliance with, the EU-U.S. Privacy Shield Framework agreed upon by the U.S. and the European Union (“EU”). The Privacy Shield Framework allows U.S. companies to receive personal data transferred from the EU without violating EU law. The Framework consists of a set of principles and related requirements that have been deemed by the European Commission as providing “adequate” privacy protection. The principles include notice; choice; accountability for onward transfer; security; data integrity and purpose limitation; access; and recourse, enforcement, and liability. The related requirements include, for example, securing an independent recourse mechanism to handle any disputes about how the company manages information about EU citizens.

To participate in the Privacy Shield Framework, a company must comply with the Privacy Shield principles and self-certify its compliance to the U.S. Department of Commerce (“Commerce”). Commerce reviews companies’ self-certification applications and maintains a public website, <https://www.privacyshield.gov/list>, where it posts the names of companies that have completed the requirements for certification. Companies are required to recertify every year in order to continue benefitting from Privacy Shield.

NTT Global provides secure data centers for housing its clients’ servers (called colocation services) and related services. In a four-count complaint, the Commission alleged that NTT Global violated Section 5(a) of the Federal Trade Commission Act by falsely representing in its privacy policy, published on its website at <http://www.ragingwire.com>, and in various marketing materials that it was a self-certified participant in, and that it complied with, the Privacy Shield Framework when it did not.

Specifically, the complaint alleged that NTT Global continued to represent that it was a Privacy Shield participant after allowing its certification to lapse. The complaint

also alleged that NTT Global failed to comply with three substantive Privacy Shield requirements by not: a) providing an independent recourse mechanism for the entire time it was a Privacy Shield participant; b) annually verifying that its assertions regarding its Privacy Shield practices were implemented and in accord with the Privacy Shield principles; and c) affirming or verifying, after it was withdrawn from the Framework, that it would delete or return information collected or that it would continue its ongoing commitment to protect any retained data it had received pursuant to Privacy Shield.

Part I of the proposed order prohibits NTT Global from making misrepresentations about its membership in any privacy or security program sponsored by the government or any other self-regulatory or standard-setting organization, including, but not limited to, the EU-U.S. Privacy Shield Framework, the Swiss-U.S. Privacy Shield Framework, and the Asia-Pacific Economic Cooperation (“APEC”) Privacy Framework.

Part II of the proposed order requires that, for so long as NTT Global participates in Privacy Shield, it must obtain an annual compliance review from a third party assessor that demonstrates that NTT Global’s assertions related to its Privacy Shield practices were implemented and are in accord with the Privacy Shield principles. The third-party assessor must be approved by the Associate Director of the Division of Enforcement of the FTC’s Bureau of Consumer Protection, and must sign a statement verifying the successful completion of each annual compliance review.

Part III of the proposed order requires that, in the case of any future lapse in NTT Global’s Privacy Shield certification, the company affirm to Commerce that it will continue to apply the Privacy Shield Framework principles to any data it received pursuant to the Framework, protect the data by another means authorized under EU or Swiss law, or delete or return such data.

Parts IV through VII of the proposed order are reporting and compliance provisions. Part IV requires acknowledgement of the order and dissemination of the order now and in the future to persons with responsibilities relating to the subject matter of the order. Part V ensures notification to the FTC of changes in corporate status and mandates that the company submit an initial compliance report to the FTC. Part VI requires the company to create and retain certain documents relating to its compliance with the order. Part VII mandates that the company make available to the FTC information or subsequent compliance reports, as requested.

The order will generally last for twenty (20) years.

The purpose of this analysis is to aid public comment on the proposed order. It is not intended to constitute an official interpretation of the complaint or proposed order, or to modify in any way the proposed order’s terms.