[BILLING CODE: 6750-01P]

FEDERAL TRADE COMMISSION

[File No. 182 3189]

RagingWire Data Centers, Inc.; Analysis to Aid Public Comment

AGENCY: Federal Trade Commission.

ACTION: Proposed Consent Agreement; Request for Comment.

SUMMARY: The consent agreement in this matter settles alleged violations of federal law prohibiting unfair or deceptive acts or practices. The attached Analysis to Aid Public Comment describes both the allegations in the complaint and the terms of the consent order—embodied in the consent agreement—that would settle these allegations.

DATES: Comments must be received on or before [INSERT DATE 30 DAYS AFTER PUBLICATION IN THE *FEDERAL REGISTER*].

ADDRESSES: Interested parties may file comments online or on paper by following the instructions in the Request for Comment part of the **SUPPLEMENTARY INFORMATION** section below. Write "RagingWire Data Centers, Inc.; File No. 182 3189" on your comment, and file your comment online at https://www.regulations.gov by following the instructions on the web-based form. If you prefer to file your comment on paper, mail your comment to the following address: Federal Trade Commission, Office of the Secretary, 600 Pennsylvania Avenue NW, Suite CC-5610 (Annex D), Washington, DC 20580, or deliver your comment to the following address: Federal Trade Commission, Office of the Secretary, Constitution Center, 400 7th Street SW, 5th Floor, Suite 5610 (Annex D), Washington, DC 20024.

FOR FURTHER INFORMATION CONTACT: Linda Holleran Kopp (202-326-2267), Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580.

SUPPLEMENTARY INFORMATION: Pursuant to Section 6(f) of the Federal Trade Commission Act, 15 U.S.C. 46(f), and FTC Rule 2.34, 16 CFR § 2.34, notice is hereby given that the above-captioned consent agreement containing a consent order to cease and desist, having been filed with and accepted, subject to final approval, by the Commission, has been placed on the public record for a period of thirty (30) days. The following Analysis to Aid Public Comment describes the terms of the consent agreement and the allegations in the complaint. An electronic copy of the full text of the consent agreement package can be obtained from the FTC Website (for June 30, 2020), at this web address: https://www.ftc.gov/news-events/commission-actions.

You can file a comment online or on paper. For the Commission to consider your comment, we must receive it on or before [INSERT DATE 30 DAYS AFTER PUBLICATION IN THE *FEDERAL REGISTER*]. Write "RagingWire Data Centers, Inc.; File No. 182 3189" on your comment. Your comment—including your name and your state—will be placed on the public record of this proceeding, including, to the extent practicable, on the https://www.regulations.gov website.

Due to the public health emergency in response to the COVID-19 outbreak and the agency's heightened security screening, postal mail addressed to the Commission will be subject to delay. We strongly encourage you to submit your comments online through the https://www.regulations.gov website.

If you prefer to file your comment on paper, write "RagingWire Data Centers, Inc.; File No. 182 3189" on your comment and on the envelope, and mail your comment to the following address: Federal Trade Commission, Office of the Secretary, 600 Pennsylvania Avenue NW, Suite CC-5610 (Annex D), Washington, DC 20580; or deliver your comment to the following address: Federal Trade Commission, Office of the Secretary, Constitution Center, 400 7th Street SW, 5th Floor, Suite 5610 (Annex D), Washington, DC 20024. If possible, submit your paper comment to the Commission by courier or overnight service.

Because your comment will be placed on the publicly accessible website at https://www.regulations.gov, you are solely responsible for making sure your comment does not include any sensitive or confidential information. In particular, your comment should not include any sensitive personal information, such as your or anyone else's Social Security number; date of birth; driver's license number or other state identification number, or foreign country equivalent; passport number; financial account number; or credit or debit card number. You are also solely responsible for making sure your comment does not include sensitive health information, such as medical records or other individually identifiable health information. In addition, your comment should not include any "trade secret or any commercial or financial information which . . . is privileged or confidential"—as provided by Section 6(f) of the FTC Act, 15 U.S.C. 46(f), and FTC Rule 4.10(a)(2), 16 CFR 4.10(a)(2)—including in particular competitively sensitive information such as costs, sales statistics, inventories, formulas, patterns, devices, manufacturing processes, or customer names.

Comments containing material for which confidential treatment is requested must be filed in paper form, must be clearly labeled "Confidential," and must comply with FTC Rule 4.9(c). In particular, the written request for confidential treatment that accompanies the comment must include the factual and legal basis for the request, and must identify the specific portions of the comment to be withheld from the public record. *See* FTC Rule 4.9(c). Your comment will be kept confidential only if the General Counsel grants your request in accordance with the law and the public interest. Once your comment has been posted on the public FTC Website—as legally required by FTC Rule 4.9(b)—we cannot redact or remove your comment from the FTC Website, unless you submit a confidentiality request that meets the requirements for such treatment under FTC Rule 4.9(c), and the General Counsel grants that request.

Visit the FTC Website at http://www.ftc.gov to read this Notice and the news release describing the proposed settlement. The FTC Act and other laws that the Commission administers permit the collection of public comments to consider and use in this proceeding, as appropriate. The Commission will consider all timely and responsive public comments that it receives on or before [INSERT DATE 30 DAYS AFTER PUBLICATION IN THE *FEDERAL REGISTER*]. For information on the Commission's privacy policy, including routine uses permitted by the Privacy Act, see https://www.ftc.gov/site-information/privacy-policy.

Analysis of Proposed Consent Order to Aid Public Comment

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 *https://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.

By direction of the Commission, Commissioner Chopra dissenting, Commissioner Slaughter not participating.

April J. Tabor,

Secretary.

Majority Statement of Chairman Joseph J. Simons and Commissioners Noah Joshua Phillips and Christine S. Wilson in the Matter of NTT Global Data Centers Americas, Inc.

The Federal Trade Commission remains committed to enforcing the EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield programs, and the order we approve today is consistent with that commitment. This order is, in fact, more protective of the Privacy Shield Principles than the 14 orders this Commission (including Commissioner Chopra) has approved in prior Privacy Shield cases. Specifically, it requires Respondent to obtain third-party assessments for as long as it participates in Privacy Shield.

Notably, this heightened obligation exceeds the scope of the notice order that the Commission (including Commissioner Chopra) unanimously approved in November 2019 in this case. Commissioner Chopra asserts that new facts have emerged in litigation that would support even more relief. But what staff did here is obtain additional evidence, through discovery, that supports the complaint's allegations. The Commission had reason to believe that Respondent's Privacy Shield representations were included in a variety of

publications and were material when we voted to litigate. During litigation, staff uncovered further evidence confirming materiality. This should not have come as a surprise to Commissioner Chopra. For example, the complaint specifically alleges that Respondent claimed, both in its privacy policy and in marketing materials, that it participated in Privacy Shield, and staff found evidence that Respondent was, in fact, touting its participation in Privacy Shield as a selling point.

Commissioner Chopra would ask us to reject a settlement that protects consumers and furthers our Privacy Shield goals, to instead continue litigation during an ongoing pandemic. There is no need and doing so would unnecessarily divert resources from other important matters, including investigations of other substantive violations of Privacy Shield. We do not support moving the goalposts in this manner[1] and for this reason vote to accept the settlement, which not just accords with but exceeds the relief the Commission unanimously sought to obtain at the outset of the case.

Dissenting Statement of Commissioner Rohit Chopra
Regarding the EU-U.S. Privacy Shield Framework in the Matter of
NTT Global Data Centers Americas, Inc.

Summary

- American businesses that participate in the EU-U.S. Privacy Shield Framework should not have to compete with those that break their privacy promises.

[1] Commissioner Chopra attempts to distinguish his earlier approval of settlements by arguing that additional relief is warranted in cases involving large businesses that violate substantive provisions of Privacy Shield. Notably, however, several recent settlements approved unanimously by this Commission that similarly alleged substantive violations of Privacy Shield involved companies that also generated substantial revenue, nor have the allegations or the defendant changed since the Commission initially approved the notice order.

- The FTC charged a data center company with violating their Privacy Shield commitments, but our proposed settlement does not even attempt to adequately remedy the harm to the market.
- The evidence in the record raises serious concerns that customers looking to follow the law relied on the company's representations and may be locked into long-term contracts.
- A quick settlement with a small firm for an inadvertent mistake may be appropriate, but it is inadequate for a dishonest, large firm violating a core pillar of Privacy Shield.
- We must consider seeking additional remedies, including rights to renegotiate contracts, disgorgement of ill-gotten revenue and data, and notice and redress for customers.

EU-U.S. Privacy Shield Framework

European companies seeking to comply with data protection rules need to ensure that their service providers are on the right side of the law. To adhere to legal requirements when transferring personal data from Europe to the United States, these companies prefer to work with partners that participate in the EU-U.S. Privacy Shield Framework, the cross-border data-sharing protocol between the European Union and the United States. One of the ways that American companies can distinguish themselves to prospective clients in the European Union is to participate (or work with a participant) in the Privacy Shield program, administered by the U.S. Department of Commerce. By participating, American companies must comply with a list of requirements on data protection, and they agree to be held accountable for these commitments. For example,

companies must articulate how individuals can access the personal data held by the participating company, explain the ways in which individuals can limit the use and disclosure of their personal data, and provide individuals access, at no charge, to an independent recourse mechanism to resolve disputes. Importantly, the Federal Trade Commission can take enforcement actions against companies that violate their Privacy Shield promises.

Strengthening the FTC Cross-Border Data Transfer Enforcement Program

Typically, the FTC uses this enforcement authority by entering into no-money, no-fault settlements where a company simply agrees it will stop breaking the law. I believe it is critical that we approach our enforcement program with a mindset of seeking continuous improvement, given the integral role we play to root out deception in this arena.

Deception does not simply harm consumers; it also harms honest businesses and it distorts fair competition. This is not a new concept – it is longstanding policy. I continue to believe that our Privacy Shield enforcement program can do more to protect and redress individuals in the European Union, while also ensuring honest American firms participating in the Privacy Shield program do not have to compete with companies that break their privacy promises.[1]

The FTC Act permits the Commission to issue orders to companies after serving notice of its charges and offering the individual or company an opportunity to respond.

---

[1] In 1983, even as the Federal Trade Commission formally adopted a more lenient posture toward deception, the FTC Policy Statement on Deception noted that the prohibition on deceptive practices is "intended to prevent injury to competitors as well as to consumers….Deceptive practices injure both competitors and consumers because consumers who preferred the competitor's product are wrongly diverted." *FTC Statement on Deception*, 103 F.T.C. 174 (1983) (appended to *Cliffdale Assocs., Inc.*, 103 F.T.C. 110, 174 (1984)), available at *https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf*.

Under our procedures, after the Commission charges a respondent with wrongdoing, the parties can exchange evidence in the discovery process and an Administrative Law Judge ultimately presides over a trial. At the conclusion of these procedures, whether through appeal or directly, the Commission can issue an order to the Respondent if the Commission concludes that there was a law violation.

But the process does not end there. After entering an order, the Commission can obtain additional remedies from a federal court if we have reason to believe that the misconduct was "dishonest" or "fraudulent."[2] These remedies include monetary restitution and rescission of contracts. In an administrative settlement, the Commission can obtain the full range of these remedies, since it is forgoing further litigation in federal court.

FTC's Administrative Complaint and Proposed Settlement with NTT

I have long been concerned with the FTC's Privacy Shield enforcement strategy, which overwhelmingly targets small businesses, some of whom may have made inadvertent mistakes. But these mistakes were still violations of law, and most of these orders did not involve violations of substantive protections of the Privacy Shield framework, so I have supported quick settlements with these small businesses given our limited resources. However, the FTC encountered a very different situation with a major data center company.

In November 2019, the Commission charged NTT Global Data Centers Americas (NTT), a major data center company controlled by Nippon Telephone & Telegraph

---

[2] Under 15 U.S.C. 57b, "[i]f the Commission satisfies the court that the act or practice to which the cease and desist order relates is one which a reasonable man would have known under the circumstances was dishonest or fraudulent," it can seek "rescission or reformation of contracts, the refund of money or return of property, the payment of damages, and public notification[.]"

formerly known as RagingWire, with failing to live up to its promises under the EU-U.S. Privacy Shield Framework. The Commission alleged that the company misrepresented its Privacy Shield participation and failed to meet certain obligations when it was a participant, including one of the core pillars: providing users with the ability to file complaints and disputes about their personal data. An administrative proceeding commenced, and NTT denied most of the Commission's allegations.[3]

The Commission now proposes to end the administrative litigation through a no-money, no-fault settlement that does not include any of the additional remedies available under the FTC Act for "dishonest" conduct. I believe the proposed settlement should be renegotiated, given that the additional evidence gathered suggests that the company's conduct was dishonest.

It is clear that the company's misrepresentations about Privacy Shield were not limited to a reference in its privacy policy. Most importantly, there was clear evidence of reliance on NTT's representations regarding its privacy protocols as a prerequisite for purchasing. Take the example of a customer of NTT, DreamHost, which offers web hosting services. DreamHost clearly values privacy. It carefully vets its partners to ensure compliance with the EU's General Data Protection Regulation. DreamHost specifically checks to see whether a prospective partner is a Privacy Shield participant. If not, DreamHost must take other steps to ensure that it meets its data protection obligations. The evidence in the record suggests that DreamHost is locked into a five-year contract

---

[3] Answer and Affirmative Defenses of Respondent Raging Wire Data Centers, LLC, NTT Global Data Centers Americas, Inc., Docket No. 9386 (Nov. 25, 2019), *https://www.ftc.gov/system/files/documents/cases/d09386_nov_25-r_answer_and_affirmative_defensepublic596761.pdf*. In its answer, the company denied that it disseminated sales materials touting its participation in Privacy Shield. Answer ¶¶ 20-21.

that will not expire until 2022.[4] Making matters worse, **[non-public information redacted]**. In other words, NTT's deception and dishonesty appears to have generated sales from customers who were seeking to protect customer privacy. This distorted the market, as NTT's competitors likely lost sales due to the alleged deception.

The proposed settlement does nothing for companies that put a premium on privacy, like DreamHost. A more appropriate settlement would include redress for customers, forfeiture of the company's gains from any deceptive sales practices, or a specific admission of liability that would allow its customers to pursue claims in private litigation. Perhaps most importantly, NTT customers that entered into long-term contracts should be free to renegotiate or terminate these agreements if they were finalized during the period when NTT was engaged in the alleged deceptive conduct. Companies like DreamHost should not be locked into long-term contracts with NTT, given the evidence of dishonest conduct. Contract remedies would allow customers to switch to NTT's law-abiding Privacy Shield-compliant competitors, who may have lost business due to the deception. Even if the Commission sought one or more of these remedies and NTT subsequently declined to agree, it would have been more prudent to resume the administrative litigation,[5] at an appropriate time.[6]

For these reasons, I respectfully dissent.

---

[4] See Declaration of Christopher Ghazarian, NTT Global Data Centers Americas, Inc., Docket No. 9386 (Dec. 20, 2019).

[5] As noted earlier, if the Commission entered a final cease-and-desist order at the conclusion of litigation, I believe this could trigger civil penalties, pursuant to Section 5(m)(1)(B) of the FTC Act, for other companies with knowledge of the order that do not fulfill their obligations under the EU-U.S. Privacy Shield Framework or other privacy or security programs sponsored by the government or a standard-setting organization. In addition, there is a paucity of litigated FTC cases in the data protection arena, which hampers development of the law.

[6] While I have great faith that our staff would be able to successfully renegotiate the existing no-money, no-fault settlement, I would be willing to continue the administrative proceeding at some time in the future. The Commission has voted to issue a number of orders to pause administrative proceedings, given the safety and logistical concerns associated with the current pandemic.

[FR Doc. 2020-14782 Filed: 7/8/2020 8:45 am; Publication Date: 7/9/2020]