

Complaint

IN THE MATTER OF

NTT GLOBAL DATA CENTERS AMERICAS, INC.**F/K/A****RAGINGWIRE DATA CENTERS, INC.**CONSENT ORDER, ETC. IN REGARD TO ALLEGED VIOLATIONS OF SECTION 5 OF THE FEDERAL
TRADE COMMISSION ACT*Docket No. 9386; File No. 182 3189**Complaint, November 5, 2019 – Decision, October 28, 2020*

This consent order addresses NTT Global Data Centers Americas, Inc., formerly known as RagingWire Data Centers, Inc.'s representations concerning its participation in, and compliance with, the EU-U.S. Privacy Shield Framework agreed upon by the U.S. and the European Union. The complaint alleges that NTT Global continued to represent that it was a Privacy Shield participant after allowing its certification to lapse. The complaint also alleges 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were implemented and in accord with the Privacy Shield principles; and c) affirming or verifying, after it was withdrawn from the Framework, that it would delete or return information collected or that it would continue its ongoing commitment to protect any retained data it had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. The consent 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 Privacy Framework.

Participants

For the *Commission*: Brian Berggren, Linda Holleran Kopp, Cathlin Tully, and Robin Wetherill.

For the *Respondents*: Corey W. Roush, Diana Schaffner, and C. Fairley Spillman, Akin Gump Strauss Hauer & Feld.

COMPLAINT

The Federal Trade Commission ("FTC"), having reason to believe that RagingWire Data Centers, Inc., a corporation, has violated the Federal Trade Commission Act ("FTC Act"), and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent RagingWire Data Centers, Inc. ("RagingWire") is a Nevada corporation with its principal office or place of business at 200 S. Virginia Street, 8th Floor, Reno, NV 89501.

2. RagingWire provides data colocation services. Specifically, RagingWire offers specialized storage facilities—often referred to as "data centers"—that are designed to house and protect servers owned and operated by other businesses, along with various complementary services including on-site technical support, network connectivity, and physical security.

Complaint

3. The acts and practices of RagingWire as alleged in this complaint have been in or affecting commerce, as “commerce” is defined in Section 4 of the FTC Act.

4. As described in more detail below, RagingWire has made deceptive statements on its website, <https://www.ragingwire.com/content/online-privacy-policy>, and in its marketing materials, about its participation in and compliance with the EU-U.S. Privacy Shield Framework and/or EU-U.S. Safe Harbor Framework.

Personal Data Transfers Under EU Law

5. The EU-U.S. Privacy Shield Framework (“Privacy Shield”) was negotiated by the Department of Commerce (“Commerce”) and the European Commission (“EC”) to provide a mechanism for companies to transfer personal data from the European Union (“EU”) to the U.S. in a manner consistent with the requirements of European Union law on data protection. Enacted in 1995, the EU Data Protection Directive set forth EU requirements for the protection of personal data. Among other things, it required EU Member States to implement legislation that prohibits the transfer of personal data outside the EU, with exceptions, unless the European Commission has made a determination that the recipient jurisdiction’s laws ensure the protection of such personal data. This determination is referred to commonly as meeting the EU’s “adequacy” standard.

6. The EU has since enacted a new data protection regime, the General Data Protection Regulation (“GDPR”), which took effect as of May 25, 2018, and contains similar provisions on data transfers. The GDPR explicitly recognizes EC adequacy determinations in effect as of that date. Unlike the Directive, the GDPR is directly applicable and generally does not require member states to enact implementing legislation.

7. To satisfy the EU adequacy standard for certain commercial transfers, Commerce and the European Commission negotiated the EU-U.S. Privacy Shield Framework, which the European Commission determined was adequate by written decision in July 2016, and took effect August 1, 2016. Thus, the EU-U.S. Privacy Shield Framework allows for the transfer of personal data lawfully from the EU to those companies in the United States that participate in Privacy Shield.

8. The EU-U.S. Privacy Shield Framework replaced the U.S.-EU Safe Harbor Framework (“Safe Harbor Framework”), in effect from 2000-2016, as a lawful mechanism under EU law for transferring data from the EU to the United States.

9. To join the EU-U.S. Privacy Shield Framework, a company must self-certify to Commerce that it complies with the Privacy Shield Principles, and to related requirements that have been deemed to meet the EU’s adequacy standard. Participating companies must annually recertify their compliance.

10. The EU-U.S. Privacy Shield Framework expressly provides that while decisions by organizations to “enter the Privacy Shield are entirely voluntary, effective compliance is compulsory: organizations that self-certify to the Department and publicly declare their

Complaint

commitment to adhere to the Principles must comply fully with the Principles.” (Emphasis added.)

11. To comply with the Privacy Shield Principles, companies must, among other things, ascertain that any third-party agents to which they transfer data received pursuant to Privacy Shield are obligated to provide at least the same level of privacy protection as is required by the Principles, as required by Privacy Shield Principle 3, “Accountability for Onward Transfer.” One way to meet this requirement is to use an agent that is also a Privacy Shield participant.

12. Companies under the jurisdiction of the FTC are eligible to join the EU-U.S. Privacy Shield Framework. The framework expressly warns companies that claim to have self-certified to the Privacy Shield Principles that failure to comply or otherwise to “fully implement” the Privacy Shield Principles “is enforceable under Section 5 of the Federal Trade Commission Act.”

13. The European Commission’s adequacy decision expressly notes that, “to ensure the proper application of the EU-U.S. Privacy Shield Framework, interested parties, such as data subjects, data exporters and the national Data Protection Authorities (DPAs), must be able to identify those organisations adhering to the Principles.” To that end, Commerce maintains a public website, <https://www.privacyshield.gov>, where it posts the names of companies that have self-certified to the EU-U.S. Privacy Shield Framework. The listing of companies, available at <https://www.privacyshield.gov/list>, indicates whether the company’s self-certification is current. A U.S. company may only benefit from the EC adequacy decision while it is on the Department of Commerce’s Privacy Shield list.

14. Under Article 83 of GDPR, transfers of personal information from the European Economic Area (“EEA”) to the United States without the benefit of an authorized mechanism such as Privacy Shield are subject to severe penalties, including administrative fines of up to 20,000,000€ or 4% of the transferor’s worldwide annual turnover from the preceding financial year, whichever is greater.

15. RagingWire is under the jurisdiction of the FTC.

RagingWire’s Business Practices

16. RagingWire offers colocation services that store customer data at one of three data centers located in the United States. RagingWire customers that collect or process personal information from the EEA and want to transfer that data to RagingWire in the U.S. can comply with GDPR and/or their own Privacy Shield obligations if RagingWire participates in Privacy Shield.

17. RagingWire originally participated in the Safe Harbor Framework, and submitted its final annual recertification for the Safe Harbor Framework on June 16, 2016.

Complaint

18. RagingWire submitted a Privacy Shield self-certification application in approximately October 2016. It obtained Privacy Shield certification in January 2017.

19. One year later, RagingWire did not complete the steps necessary to renew its Privacy Shield certification, and its Privacy Shield certification lapsed in January 2018.

20. From approximately January 2017 until October 2018, RagingWire disseminated or caused to be disseminated the following representations in its online privacy policy, available at <https://www.ragingwire.com/content/online-privacy-policy>, including, but not limited to, statements that it participated in and complied with the EU-U.S. Privacy Shield (the “Privacy Shield Statements”):

EU-U.S. Privacy Shield

RagingWire complies with the EU-US Privacy Shield Framework as set forth by the US Department of Commerce regarding the collection, use, and retention of personal information from European Union member countries. RagingWire has certified that it adheres to the Privacy Shield Principles of Notice, Choice, Accountability for Onward Transfer, Security, Data Integrity and Purpose Limitation, Access, and Recourse, Enforcement and Liability. If there is any conflict between the policies in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification page, please visit <https://www.privacyshield.gov/>

The Federal Trade Commission (FTC) has jurisdiction over RagingWire’s compliance with the Privacy Shield.

DISPUTE RESOLUTION

In compliance with the EU-US Privacy Shield Principles, RagingWire commits to resolve complaints about your privacy and our collection or use of your personal information. . . . If you have an unresolved privacy or data use concern that we have not addressed satisfactorily, please contact our U.S.-based third party dispute resolution provider (free of charge) at <https://feedback-form.truste.com/watchdog/request>. Please note that if your complaint is not resolved through these channels, under limited circumstances, a binding arbitration option may be available before a Privacy Shield Panel.

21. RagingWire also has disseminated or caused to be disseminated sales materials containing representations that RagingWire was a participant in Privacy Shield and/or the Safe Harbor Framework after it was no longer participating in the frameworks. For example, RagingWire’s marketing slides, the “Sales Tour Deck,” represented in 2018 that RagingWire participated in the Safe Harbor Framework when, in fact, RagingWire no longer participated in the Safe Harbor Framework or Privacy Shield as of January 2018. A copy of this representation is attached hereto as Exhibit A.

Complaint

22. Following the lapse of RagingWire's Privacy Shield certification in January 2018, Commerce warned the company in February 2018, and again in May 2018, to take down its claims that it participated in Privacy Shield unless and until such time as it completed the steps necessary to renew its participation in the EU-U.S. Privacy Shield Framework.

23. RagingWire did not remove its Privacy Shield Statements until October 2018, after RagingWire was contacted by the FTC.

24. In June 2019, RagingWire again obtained Privacy Shield certification.

RagingWire's Privacy Shield Non-Compliance

25. At least during the January 2017-18 period that RagingWire was a Privacy Shield participant, RagingWire failed to comply with the Privacy Shield Principles.

RagingWire's Failure to Verify Compliance

26. Supplemental Principle 7 of the Privacy Shield Principles requires any company that participates in Privacy Shield to annually verify, through self-assessment or outside compliance review, that the assertions it makes about its Privacy Shield privacy practices are true and that those privacy practices have been implemented.

27. Participants must also prepare a statement, signed by a corporate officer or outside reviewer, that such assessment or outside compliance review has been completed. Participants must make their annual verification statements available on request to the FTC or Department of Transportation, whoever has unfair and deceptive practices jurisdiction over the company.

28. During the 2017-18 period that RagingWire participated in Privacy Shield, RagingWire did not verify, through self-assessment or outside compliance review, that its assertions about its Privacy Shield privacy practices were true and that those privacy practices had been implemented.

29. During the 2017-18 period that RagingWire participated in Privacy Shield, RagingWire also did not complete a verification statement signed by an officer or outside compliance reviewer that the assertions it had made about its Privacy Shield privacy practices during the time it participated in the program were true and that those privacy practices had been implemented.

RagingWire's Failure to Maintain an Independent Recourse Mechanism

30. Principle 7(a)(i) of the Privacy Shield Principles requires, among other things, that organizations participating in Privacy Shield provide "readily available independent recourse mechanisms by which each individual's complaints and disputes are investigated and expeditiously resolved at no cost to the individual and by reference to the Principles."

Complaint

Supplemental Principle 11(a) specifies that participating organizations may comply with Principle 7(a)(i) by using a qualifying private-sector program.

31. TRUSTe LLC (“TRUSTe”), a subsidiary of TrustArc Inc., offers a qualifying Privacy Shield dispute resolution mechanism. Privacy Shield participants may satisfy the requirements of Principle 7(a)(i) and Supplemental Principle 11(a) by participating in TRUSTe’s dispute resolution program.

32. RagingWire contracted with TRUSTe to provide dispute resolution services.

33. Under the heading “Dispute Resolution,” RagingWire’s Privacy Shield Statements included a hyperlink to the private sector program developed by TRUSTe LLC. RagingWire’s Privacy Shield Statements directed consumers to use that link to submit “unresolved privacy or data use concern[s]” to RagingWire’s “U.S.-based third party dispute resolution provider.”

34. However, RagingWire’s subscription with TRUSTe was terminated as of October 1, 2017, and TRUSTe ceased providing dispute resolution services to RagingWire as of that date. RagingWire did not renew its dispute resolution subscription with TRUSTe until June 2018.

RagingWire’s Failure to Properly Withdraw and Affirm Its Ongoing Compliance

35. Supplemental Principle 6(f) of the Privacy Shield Principles requires that any participant that withdraws from Privacy Shield affirm to Commerce that it will either continue to apply the Privacy Shield Principles to any data received pursuant to Privacy Shield or will delete or return all such data. Supplemental Principle 7 requires organizations to respond promptly to inquiries and other requests for information from Commerce relating to the organization’s adherence to the Privacy Shield Principles.

36. In February 2018, Commerce informed RagingWire that, because its certification had lapsed, it was required to complete a questionnaire verifying whether the company would re-certify or withdraw from the program and, if the latter, whether RagingWire would return and delete the data it had received under Privacy Shield or would continue to apply the Privacy Shield Principles to that data.

37. RagingWire did not complete the questionnaire.

Count 1-Privacy Shield Participation Misrepresentation

38. As described in Paragraphs 20-21, RagingWire has represented, directly or indirectly, expressly or by implication, that it was a current participant in the EU-U.S Privacy Shield Framework and/or the Safe Harbor Framework from at least January 2017 until at least October 2018.

39. In fact, as described in Paragraphs 17 and 19, RagingWire’s Privacy Shield and Safe Harbor Framework certifications had lapsed and it was not a current participant in the EU-

Complaint

U.S. Privacy Shield Framework or the Safe Harbor Framework from at least January 2018 until approximately June 2019. Therefore, the representations set forth in Paragraphs 38 were false or misleading.

Count 2-Misrepresentation Regarding Verification

40. As described in Paragraphs 20-21, RagingWire has represented, directly or indirectly, expressly or by implication, that it complies with the Privacy Shield Principles.

41. In fact, as described in Paragraphs 26-29, RagingWire failed to comply with the verification requirements during the time it participated in Privacy Shield. Therefore, the representations set forth in Paragraph 40 were false or misleading.

Count 3-Misrepresentation Regarding Dispute Resolution

42. As described in Paragraphs 20-21, RagingWire has represented, directly or indirectly, expressly or by implication, that it complies with the Privacy Shield Principles.

43. In fact, as described in Paragraphs 30-34, RagingWire failed to comply with the Privacy Shield Principles' requirement that it maintain a readily available independent recourse mechanism for the period from approximately October 1, 2017 through June 19, 2018. Therefore, the representations set forth in Paragraph 42 were false or misleading.

Count 4-Misrepresentation Regarding Continuing Obligations

44. As described in Paragraphs 20-21, RagingWire has represented, directly or indirectly, expressly or by implication, that it complies with the Privacy Shield Principles.

45. In fact, as described in Paragraphs 35-37, RagingWire let its certification lapse and did not affirm or verify to Commerce that it would either delete or return personal information that it received during the time it participated in the program or would continue to apply the principles to such information. Therefore, the representations set forth in Paragraph 44 were false or misleading.

Violations of Section 5 of the FTC Act

46. The acts and practices of RagingWire as alleged in this complaint constitute deceptive acts or practices, in or affecting commerce, in violation of Section 5(a) of the Federal Trade Commission Act.

NOTICE

You are notified that on the seventh day of July, 2020, at 10:00 a.m., at the Federal Trade Commission offices, 600 Pennsylvania Avenue, NW, Room 532-H, Washington, DC 20580, an Administrative Law Judge of the Federal Trade Commission, will hold a hearing on the charges set forth in this Complaint. At that time and place, you will have the right under the Federal

Complaint

Trade Commission Act to appear and show cause why an order should not be entered requiring you to cease and desist from the violations of law charged in this Complaint.

You are notified that you are afforded the opportunity to file with the Federal Trade Commission (“Commission”) an answer to this Complaint on or before the 14th day after service of the Complaint upon you. An answer in which the allegations of the Complaint are contested must contain a concise statement of the facts constituting each ground of defense; and specific admission, denial, or explanation of each fact alleged in the Complaint or, if you are without knowledge thereof, a statement to that effect. Allegations of the Complaint not thus answered will be deemed to have been admitted.

If you elect not to contest the allegations of fact set forth in the Complaint, the answer should consist of a statement that you admit all of the material facts to be true. Such an answer will constitute a waiver of hearings as to the facts alleged in the Complaint and, together with the Complaint, will provide a record basis on which the Commission may issue a final decision containing appropriate findings and conclusions and a final order disposing of the proceeding. In such answer, you may, however, reserve the right to submit proposed findings of fact and conclusions of law under FTC Rule § 3.46.

Failure to answer timely will be deemed to constitute a waiver of your right to appear and contest the allegations of the Complaint. It will also authorize the Commission, without further notice to you, to find the facts to be as alleged in the Complaint and to enter a final decision containing appropriate findings and conclusions and a final order disposing of the proceeding.

The Administrative Law Judge will hold an initial prehearing scheduling conference to be held not later than 10 days after the answer is filed by the Respondent. Unless otherwise directed by the Administrative Law Judge, the scheduling conference and further proceedings will take place at the Federal Trade Commission, 600 Pennsylvania Avenue, NW, Room 532-H, Washington, DC 20580. Rule 3.21(a) requires a meeting of the parties’ counsel as early as practicable before the prehearing scheduling conference, but in any event no later than 5 days after the answer is filed by the Respondent. Rule 3.31(b) obligates counsel for each party, within 5 days of receiving a Respondent’s answer, to make certain initial disclosures without awaiting a formal discovery request.

The following is the form of the order which the Commission has reason to believe should issue if the facts are found to be as alleged in the Complaint. If, however, the Commission concludes from record facts developed in any adjudicative proceedings in this matter that the proposed order provisions as to Respondent might be inadequate to fully protect the consuming public, the Commission may order such other relief as it finds necessary and appropriate.

Complaint

ORDER**Definitions**

For purposes of this Order, the following definition applies:

- A. “Respondent” means RagingWire Data Centers, Inc., a corporation, and its successors and assigns.

Provisions**I. Prohibition against Misrepresentations about Participation in or Compliance with Privacy Programs**

IT IS ORDERED that Respondent and its officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, in connection with the advertising, marketing, promotion, offering for sale, or sale of any product or service must not misrepresent in any manner, expressly or by implication, the extent to which Respondent is a member of, adheres to, complies with, is certified by, is endorsed by, or otherwise participates in any privacy or security program sponsored by a government or any self-regulatory or standard-setting organization, including but not limited to the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework and the APEC Cross-Border Privacy Rules.

II. Requirement to Meet Continuing Obligations Under Privacy Shield

IT IS ORDERED that Respondent and its officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, in connection with the advertising, marketing, promotion, offering for sale, or sale of any product or service, must affirm to the Department of Commerce, within thirty (30) days after any withdrawal or lapse in its certification to the EU-U.S. Privacy Shield Framework or the Swiss-U.S. Privacy Shield Framework, and on an annual basis thereafter for as long as it retains such information, that it will:

1. Continue to apply the EU-U.S. Privacy Shield Framework Principles to the personal information it received while it participated in the Privacy Shield; or
2. Protect the information by another means authorized under EU (for the EU-U.S. Privacy Shield Framework) or Swiss (for the Swiss-U.S. Privacy Shield Framework) law, including by using a binding corporate rule or a contract that fully reflects the requirements of the relevant standard contractual clauses adopted by the European Commission; or
3. Return or delete the information.

Complaint

III. Acknowledgments of the Order

IT IS FURTHER ORDERED that Respondent obtain acknowledgments of receipt of this Order:

- A. Respondent, within ten (10) days after the effective date of this Order, must submit to the Commission an acknowledgment of receipt of this Order.
- B. For twenty (20) years after the issuance date of this Order, Respondent must deliver a copy of this Order to: (1) all principals, officers, directors, and LLC managers and members; (2) all employees having managerial responsibilities for conduct related to the subject matter of the Order and all agents and representatives who participate in conduct related to the subject matter of the Order; and (3) any business entity resulting from any change in structure as set forth in the Provision titled Compliance Report and Notices. Delivery must occur within ten (10) days after the effective date of this Order for current personnel. For all others, delivery must occur before they assume their responsibilities.
- C. From each individual or entity to which Respondent delivered a copy of this Order, Respondent must obtain, within thirty (30) days, a signed and dated acknowledgment of receipt of this Order.

IV. Compliance Report and Notices

IT IS FURTHER ORDERED that Respondent make timely submissions to the Commission:

- A. Sixty (60) days after the effective date of this Order, Respondent must submit a compliance report, sworn under penalty of perjury, in which Respondent must: (a) identify the primary physical, postal, and email address and telephone number, as designated points of contact, which representatives of the Commission, may use to communicate with Respondent; (b) identify all of Respondent's businesses by all of their names, telephone numbers, and physical, postal, email, and Internet addresses; (c) describe the activities of each business; (d) describe in detail whether and how Respondent is in compliance with each Provision of this Order; and (e) provide a copy of each Acknowledgment of the Order obtained pursuant to this Order, unless previously submitted to the Commission.
- B. Respondent must submit a compliance notice, sworn under penalty of perjury, within fourteen (14) days of any change in the following: (1) any designated point of contact; or (2) the structure of Respondent or any entity that Respondent has any ownership interest in or controls directly or indirectly that may affect compliance obligations arising under this Order, including: creation, merger, sale, or dissolution of the entity or any subsidiary, parent, or affiliate that engages in any acts or practices subject to this Order.

Complaint

- C. Respondent must submit notice of the filing of any bankruptcy petition, insolvency proceeding, or similar proceeding by or against Respondent within fourteen (14) days of its filing.
- D. Any submission to the Commission required by this Order to be sworn under penalty of perjury must be true and accurate and comply with 28 U.S.C. § 1746, such as by concluding: “I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on: _____” and supplying the date, signatory’s full name, title (if applicable), and signature.
- E. Unless otherwise directed by a Commission representative in writing, all submissions to the Commission pursuant to this Order must be emailed to Debrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580. The subject line must begin: In re *RagingWire Data Centers, Inc.*, FTC File No. 1823189.

V. Recordkeeping

IT IS FURTHER ORDERED that Respondent must create certain records for twenty (20) years after the issuance date of the Order, and retain each such record for five (5) years. Specifically, Respondent must create and retain the following records:

- A. accounting records showing the revenues from all goods or services sold;
- B. personnel records showing, for each person providing services, whether as an employee or otherwise, that person’s: name; addresses; telephone numbers; job title or position; dates of service; and (if applicable) the reason for termination;
- C. all records necessary to demonstrate full compliance with each provision of this Order, including all submissions to the Commission; and
- D. a copy of each widely disseminated representation by Respondent making any representation subject to this Order, and all materials that were relied upon in making the representation.

VI. Compliance Monitoring

IT IS FURTHER ORDERED that, for the purpose of monitoring Respondent’s compliance with this Order:

- A. Within ten (10) days of receipt of a written request from a representative of the Commission, Respondent must: submit additional compliance reports or other requested information, which must be sworn under penalty of perjury, and produce records for inspection and copying.

Complaint

- B. For matters concerning this Order, representatives of the Commission are authorized to communicate directly with Respondent. Respondent must permit representatives of the Commission to interview anyone affiliated with Respondent who has agreed to such an interview. The interviewee may have counsel present.
- C. The Commission may use all other lawful means, including posing through its representatives as consumers, suppliers, or other individuals or entities, to Respondent or any individual or entity affiliated with Respondent, without the necessity of identification or prior notice. Nothing in this Order limits the Commission's lawful use of compulsory process, pursuant to Sections 9 and 20 of the FTC Act, 15 U.S.C. §§ 49, 57b-1.

VII. Order Effective Dates

IT IS FURTHER ORDERED that the final and effective date of this Order is the 60th day after this Order is served. This Order will terminate twenty (20) years from the date of its issuance (which date may be stated at the end of this Order, near the Commission's seal), or twenty (20) years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying settlement) in federal court alleging any violation of the Order, whichever comes later; *provided, however*, that the filing of such a complaint will not affect the duration of:

- A. any Provision in this Order that terminates in less than twenty (20) years;
- B. this Order's application to any respondent that is not named as a defendant in such complaint; and
- C. this Order if such complaint is filed after the order has terminated pursuant to this Provision.

Provided, further, that if such complaint is dismissed or a federal court rules that Respondent did not violate any provision of the Order, and the dismissal or ruling is either not appealed or upheld on appeal, then the Order will terminate according to this Provision as though the complaint had never been filed, except that the Order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

THEREFORE, the Federal Trade Commission, this fifth day of November, 2019, has issued this Complaint against Respondent.

By the Commission.

Decision and Order

DECISION

The Federal Trade Commission (“Commission”) issued a complaint challenging certain acts and practices of the Respondent named above in the caption. The Commission’s Bureau of Consumer Protection (“BCP”) filed the Complaint, which charged the Respondent with violating the Federal Trade Commission Act.

Respondent and BCP thereafter executed an Agreement Containing Consent Order (“Consent Agreement”). The Consent Agreement includes: 1) statements by Respondent that it neither admits nor denies any of the allegations in the Complaint, except as specifically stated in this Decision and Order, and that only for purposes of this action, it admits the facts necessary to establish jurisdiction; and 2) waivers and other provisions as required by the Commission’s Rules.

The Acting Secretary of the Commission thereafter withdrew this matter from adjudication in accordance with Section 3.25(c) of the Commission’s Rules, 16 C.F.R. 3.25(c) (“Rule 3.25”).

The Commission accepted the executed Consent Agreement and placed it on the public record for a period of 30 days for the receipt and consideration of public comments. The Commission duly considered any comments received from interested persons pursuant to Rule 2.34. Now, in further conformity with the procedure prescribed in Rule § 3.25 (f), the Commission makes the following Findings and issues the following Order:

Findings

1. Respondent is NTT Global Data Centers Americas, Inc., a Nevada corporation, with its principal office or place of business at 1625 W. National Drive, Sacramento, CA 95834. NTT Global Data Centers Americas, Inc. is the successor in interest to RagingWire Data Centers, Inc.
2. The Federal Trade Commission has jurisdiction over the subject matter of this proceeding and over the Respondent, and the proceeding is in the public interest.

ORDER**Definitions**

For purposes of this Order, the following definition applies:

- A. **“Respondent”** means NTT Global Data Centers Americas, Inc., and any successors and assigns.
- B. **“EU”** means European Union.

Decision and Order

- C. **“Privacy Shield”** means the EU-U.S. Privacy Shield Framework and/or the Swiss-U.S. Privacy Shield Framework, administered by the U.S. Department of Commerce.
- D. **“Privacy Shield Principles”** means the requirements for self-certified participants of the EU-U.S. Privacy Shield Framework and/or the Swiss-U.S. Privacy Shield Framework, as reflected in Exhibit A.

Provisions**I. Prohibition Against Misrepresentations About Participation in or Compliance with Privacy Programs**

IT IS ORDERED that Respondent and its officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, in connection with the advertising, marketing, promotion, offering for sale, or sale of any product or service must not misrepresent in any manner, expressly or by implication, the extent to which Respondent is a member of, adheres to, complies with, is certified by, is endorsed by, or otherwise participates in any privacy or security program sponsored by a government or any 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 APEC Cross-Border Privacy Rules.

II. Requirement for Annual Outside Compliance Review

IT IS ORDERED that, commencing no later than 120 days after the effective date of this Order and for so long as Respondent is a self-certified participant in Privacy Shield, Respondent and its officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, in connection with the advertisement, marketing, promotion, offering for sale, or sale of any product or service, shall obtain an annual outside compliance review from an independent third-party assessor approved by the Associate Director for the Division of Enforcement of the Bureau of Consumer Protection at the Federal Trade Commission, that demonstrates that the assertions Respondent makes about its Privacy Shield practices are true, and that those Privacy Shield practices have been implemented as represented and in accord with the Privacy Shield Principles. A statement verifying that an outside compliance review has been successfully completed must be signed by the third-party assessor and made available to the Commission upon request.

III. Requirement to Meet Continuing Obligations Under Privacy Shield

IT IS ORDERED that Respondent and its officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, in connection with the advertising, marketing, promotion, offering for sale, or sale of any product or service, must affirm to the Department of Commerce, within thirty (30) days after any withdrawal or lapse in its

Decision and Order

certification to the EU-U.S. Privacy Shield Framework or the Swiss-U.S. Privacy Shield Framework, and on an annual basis thereafter for as long as it retains such information, that it will:

- A. Continue to apply the EU-U.S. Privacy Shield Framework Principles to the personal information it received while it participated in the Privacy Shield; or
- B. Protect the information by another means authorized under EU (for the EU-U.S. Privacy Shield Framework) or Swiss (for the Swiss-U.S. Privacy Shield Framework) law, including by using a binding corporate rule or a contract that fully reflects the requirements of the relevant standard contractual clauses adopted by the European Commission; or
- C. Return or delete the information.

IV. Acknowledgments of the Order

IT IS FURTHER ORDERED that Respondent obtain acknowledgments of receipt of this Order:

- A. Respondent, within ten (10) days after the effective date of this Order, must submit to the Commission an acknowledgment of receipt of this Order.
- B. For five (5) years after the issuance date of this Order, Respondent must deliver a copy of this Order to: (1) all principals, officers, directors, and LLC managers and members; (2) all employees having managerial responsibilities for conduct related to the subject matter of the Order and all agents and representatives who participate in conduct related to the subject matter of the Order; and (3) any business entity resulting from any change in structure as set forth in the Provision titled Compliance Report and Notices. Delivery must occur within ten (10) days after the effective date of this Order for current personnel. For all others, delivery must occur before they assume their responsibilities.
- C. From each individual or entity to which Respondent delivered a copy of this Order, Respondent must obtain, within thirty (30) days, a signed and dated acknowledgment of receipt of this Order.

V. Compliance Report and Notices

IT IS FURTHER ORDERED that Respondent make timely submissions to the Commission:

- A. Sixty (60) days after the effective date of this Order, Respondent must submit a compliance report, sworn under penalty of perjury, in which Respondent must: (a) identify the primary physical, postal, and email address and telephone number, as designated points of contact, which representatives of the Commission, may use

Decision and Order

to communicate with Respondent; (b) identify all of Respondent's businesses by all of their names, telephone numbers, and physical, postal, email, and Internet addresses; (c) describe the activities of each business; (d) describe in detail whether and how Respondent is in compliance with each Provision of this Order; and (e) provide a copy of each Acknowledgment of the Order obtained pursuant to this Order, unless previously submitted to the Commission.

- B. Respondent must submit a compliance notice, sworn under penalty of perjury, within fourteen (14) days of any change in the following: (1) any designated point of contact; or (2) the structure of Respondent or any entity that Respondent has any ownership interest in or controls directly or indirectly that may affect compliance obligations arising under this Order, including: creation, merger, sale, or dissolution of the entity or any subsidiary, parent, or affiliate that engages in any acts or practices subject to this Order.
- C. Respondent must submit notice of the filing of any bankruptcy petition, insolvency proceeding, or similar proceeding by or against Respondent within fourteen (14) days of its filing.
- D. Any submission to the Commission required by this Order to be sworn under penalty of perjury must be true and accurate and comply with 28 U.S.C. § 1746, such as by concluding: "I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on: _____" and supplying the date, signatory's full name, title (if applicable), and signature.
- E. Unless otherwise directed by a Commission representative in writing, all submissions to the Commission pursuant to this Order must be emailed to Debrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580. The subject line must begin: In re *NTT Global Data Centers Americas, Inc.*, Docket No. 9386.

VI. Recordkeeping

IT IS FURTHER ORDERED that Respondent must create certain records for ten (10) years after the issuance date of the Order, and retain each such record for five (5) years. Specifically, Respondent must create and retain the following records:

- A. accounting records showing the revenues from all goods or services sold;
- B. personnel records showing, for each person providing services, whether as an employee or otherwise, that person's: name; addresses; telephone numbers; job title or position; dates of service; and (if applicable) the reason for termination;

Decision and Order

- C. all records necessary to demonstrate full compliance with each provision of this Order, including all submissions to the Commission; and
- D. a copy of each widely disseminated representation by Respondent making any representation subject to this Order, and all materials that were relied upon in making the representation.

VII. Compliance Monitoring

IT IS FURTHER ORDERED that, for the purpose of monitoring Respondent's compliance with this Order:

- A. Within ten (10) days of receipt of a written request from a representative of the Commission, Respondent must: submit additional compliance reports or other requested information, which must be sworn under penalty of perjury, and produce records for inspection and copying.
- B. For matters concerning this Order, representatives of the Commission are authorized to communicate directly with Respondent. Respondent must permit representatives of the Commission to interview anyone affiliated with Respondent who has agreed to such an interview. The interviewee may have counsel present.
- C. The Commission may use all other lawful means, including posing through its representatives as consumers, suppliers, or other individuals or entities, to Respondent or any individual or entity affiliated with Respondent, without the necessity of identification or prior notice. Nothing in this Order limits the Commission's lawful use of compulsory process, pursuant to Sections 9 and 20 of the FTC Act, 15 U.S.C. §§ 49, 57b-1.

VIII. Order Effective Dates

IT IS FURTHER ORDERED that the final and effective date of this Order is the 60th day after this Order is served. This Order will terminate on October 28, 2040, or twenty (20) years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying settlement) in federal court alleging any violation of the Order, whichever comes later; *provided, however*, that the filing of such a complaint will not affect the duration of:

- A. any Provision in this Order that terminates in less than twenty (20) years;
- B. this Order's application to any respondent that is not named as a defendant in such complaint; and
- C. this Order if such complaint is filed after the order has terminated pursuant to this Provision.

Statement of the Commission

Provided, further, that if such complaint is dismissed or a federal court rules that Respondent did not violate any provision of the Order, and the dismissal or ruling is either not appealed or upheld on appeal, then the Order will terminate according to this Provision as though the complaint had never been filed, except that the Order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

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

**MAJORITY STATEMENT OF CHAIRMAN JOSEPH J. SIMONS AND
COMMISSIONERS NOAH JOSHUA PHILLIPS AND CHRISTINE S. WILSON**

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 manner¹ and for this reason vote to accept the settlement,

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

Dissenting Statement

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

June 30, 2020

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.
- 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

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.

Dissenting Statement

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. 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.

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.

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[.]”

Dissenting Statement

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 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 that will not expire until 2022.⁴ Making matters worse, [REDACTED]

[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.

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.

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

Dissenting Statement

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.

Attachment**DECLARATION OF CHRISTOPHER GHAZARIAN**

PURSUANT TO 28 U.S.C. § 1746

I, Christopher Ghazarian have personal knowledge of the following facts and matters discussed in this declaration. If called as a witness I would testify as follows:

1. I am over age 18 years old and reside in California.
2. I am the General Counsel of DreamHost, LLC ("DreamHost"). Dream Host provides a variety of webhosting services that allow customers to create websites and host them on DreamHost's servers.

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.

Dissenting Statement

3. DreamHost has housed some of those servers in facilities owned and operated by RagingWire Data Centers, Inc. (“RagingWire”). DreamHost most recently renewed its contract with RagingWire in 2017. The term of the contract is five years.

4. Starting in 2017, DreamHost started working towards meeting the requirements for GDPR compliance. DreamHost complies with GDPR, and ensures that all of its partners that deal with personally identifiable information from residents in the European Economic Area are also compliant. DreamHost vets all of its partners from security, legal and privacy standpoints, which includes checking the partner’s privacy policy.

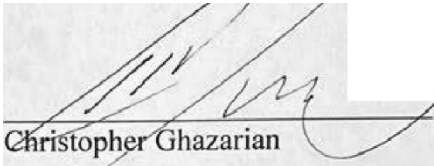
5. For partners implicated by GDPR, one of the many things we check for is to see if the partner is Privacy Shield certified. If a company is not Privacy Shield certified, we pursue other methods to ensure GDPR compliance, such as model contract clauses. The accuracy of a company’s representations about being a Privacy Shield participant is a big deal to DreamHost.

6. Working with Privacy Shield-certified partners is attractive because the partner’s certification gives us more peace of mind when considering whether or not to partner with that company. Raging Wire’s Privacy Shield certification was therefore a plus for deciding to work with RagingWire.

7. There was a discussion about DreamHost’s GDPR or Privacy Shield compliance in one of DreamHost’s community forum discussion groups on or around May 2018. A true and correct copy of a screenshot of this discussion is attached to this declaration *as* Exhibit A.

I declare under the penalty of perjury that the foregoing is true and correct.

Date: December 20, 2019



Christopher Ghazarian

Analysis to Aid Public Comment

STATEMENT OF COMMISSIONER ROHIT CHOPRA*October 28, 2020*

I respectfully dissent from today's action to give final approval to this settlement. Evidence uncovered in the litigation makes clear that businesses relied on NTT's EU-U.S. Privacy Shield promises, yet the settlement proposed does nothing to help these businesses or to meaningfully hold NTT accountable.¹ The Commission's vote to finalize another data protection settlement – with no money, no help for victims, and no admission or findings of liability – is a setback for the FTC's privacy enforcement program. I am hopeful we will change course.

I have recently outlined another way to reduce the FTC's reliance on no-consequences settlements, provide help for victims, and trigger penalties for those who engage in similar conduct.² I extend my sincere thanks to the public commenters who weighed in, in the pursuit of accountability for those that violate their Privacy Shield promises.³

ANALYSIS OF 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

1 Dissenting Statement of Commissioner Rohit Chopra Regarding the EU-U.S. Privacy Shield Framework in the Matter of NTT Global Data Centers Americas, Comm'n File No. 1823189 (Jun. 30, 2020), <https://www.ftc.gov/public-statements/2020/06/dissenting-statement-commissioner-rohit-chopra-regarding-eu-us-privacy>; Declaration of Christopher Ghazarian, NTT Global Data Centers Americas, Inc., Docket No. 9386 (Dec. 20, 2019).

2 Restating longstanding Commission policy regarding misrepresentations of affiliations with the government into a Commission rule would not create any substantive requirements for market participants, but would allow the Commission to more easily obtain appropriate remedies. Statement of Commissioner Rohit Chopra Regarding the Report to Congress on Protecting Older Consumers, Commission File No. P144400 (Oct. 19, 2020), <https://www.ftc.gov/public-statements/2020/10/statement-commissioner-rohit-chopra-regarding-report-congress-protecting>.

3 BEUC – The European Consumer Organisation, (Aug. 6, 2020), <https://beta.regulations.gov/comment/FTC-2020-0053-0002>; Burcu Kilic, on Behalf of Transatlantic Consumer Dialogue (TACD), (Aug. 10, 2020), <https://beta.regulations.gov/comment/FTC-2020-0053-0003>.

Analysis to Aid Public Comment

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.

Analysis to Aid Public Comment

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.

Complaint

IN THE MATTER OF

**SUNDAY RILEY MODERN SKINCARE, LLC,
AND
SUNDAY RILEY**CONSENT ORDER, ETC. IN REGARD TO ALLEGED VIOLATIONS OF SECTION 5 OF THE FEDERAL
TRADE COMMISSION ACT*Docket No. C-4729; File No. 192 3008**Complaint, November 6, 2020 – Decision, November 6, 2020*

This consent order addresses Sunday Riley Modern Skincare, LLC's marketing of their Sunday Riley brand cosmetic products. The complaint alleges that the respondents violated Section 5(a) of the Federal Trade Commission Act by misrepresenting that certain reviews of Sunday Riley brand products on the Sephora website reflected the independent experiences or opinions of impartial ordinary users of the products, when they were written by Ms. Riley and her employees. The complaint further alleges that the respondents deceptively failed to disclose that certain online consumer reviews were written by Ms. Riley or her employees. The consent order prohibits the respondents, in connection with the sale of any product, from misrepresenting the status of any endorser or person providing a review of the product, including misrepresenting that the endorser or reviewer is an independent or ordinary user of the product.

Participants

For the *Commission*: Michael Ostheimer.

For the *Respondents*: Behnam Dayanim, Charles A. Patrizia, and Noah N. Simmons, Paul Hastings.

COMPLAINT

The Federal Trade Commission, having reason to believe that Sunday Riley Modern Skincare, LLC, a limited liability company, and Sunday Riley, individually and as an officer of Sunday Riley Modern Skincare, LLC (collectively, "Respondents"), have violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent Sunday Riley Modern Skincare, LLC ("Sunday Riley Skincare") is a Texas limited liability company with its principal office or place of business at 4444 Westheimer Road, Suite G305, Houston, Texas 77027-4455.

2. Respondent Sunday Riley is the Chief Executive Officer of Sunday Riley Skincare. Individually or in concert with others, she controlled or had the authority to control or participated in the acts and practices of Sunday Riley Skincare, including the acts and practices alleged in this complaint. Her principal office or place of business is the same as that of Sunday Riley Skincare.