

IN-CLASS EXERCISE 2

RagingWire Data Centers, Inc., a corporation

1. Complaint and Section 5:

The FTC states about the compliance with Section 5 “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.”

Complaint summary:

- RagingWire has been affecting commerce. 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.
- 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.
- RagingWire submitted a Privacy Shield self-certification application in approximately October 2016. It obtained Privacy Shield certification in January 2017. 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.

2. Original compliant date: November 7, 2019.

3. Name of the company: NTT Global Data Centers Americas, Inc., a corporation, as successor in interest to RagingWire Data Centers, Inc., a corporation.

4. Description of Services: 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.

5. Description of FTC original compliant:

- Privacy Shield Participation Misrepresentation
- Misrepresentation Regarding Verification
- Misrepresentation Regarding Dispute Resolution
- Misrepresentation Regarding Continuing Obligations

- Violations of Section 5 of the FTC Act 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.

6. Number of consumers affected: The complaint does not specify the exact number of affected consumers. However, it suggests that because the company did not fully comply with the EU-US Privacy Shield Framework, it is reasonable to consider that all consumers could be impacted.

7. Facts of how the violation happened:

- RagingWire 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.
- 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.
- RagingWire did not remove its Privacy Shield Statements until October 2018, after RagingWire was contacted by the FTC. In June 2019, RagingWire again obtained Privacy Shield certification.
- 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.
- However, RagingWire didn’t reply to this questionnaire, which created the violation alleged by the FTC.

8. How did FTC find out?

FTC found out after Commerce informed RagingWire about the expired certification they hold. As RagingWire didn’t reply to the questions and allegations made by commerce, FTC came into play and started an in-depth investigation and filed the NOTICE on RagingWire.

9. What does the Cease and Desist order mandate?

It tries to prohibit RagingWire making misconceptions and claims of participating in or complying with privacy programs like the EU-U.S. Privacy Shield Framework.

It mandates the following:

- Should not make false claims.
- Should protect the personal information of the public or consumers after their participation lapses.
- Should provide acknowledgement of the order within 10 days.

- It should deliver the report for compliance and meet the record-keeping requirements of 20 years.

10. Order dates start and end: The order's effective date is 60 days after it is served, as stated in Section VII: "IT IS FURTHER ORDERED that the final and effective date of this order is the 60th day after this order is served."

The order will terminate 20 years from its issuance date or 20 years from the most recent date that a complaint is filed alleging any violation of the order, whichever comes later. The exact end date is not specified in the document.

11. Find instances of language “reasonable” or “at the minimum.”.

After going through the document, I was unable to find any instances mentioning specifically “reasonable” or “at the minimum”, but instead found the words up to the degree where it wants the RagingWire to comply.

Find instances of language
“Reasonable” or “At a
minimum”

An instance of the above is given below:

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.