



Office of Commissioner
Rohit Chopra

UNITED STATES OF AMERICA
Federal Trade Commission
WASHINGTON, D.C. 20580

DISSENTING STATEMENT OF COMMISSIONER ROHIT CHOPRA

*Regarding the EU-U.S. Privacy Shield Framework
in the Matter of NTT Global Data Centers Americas
Commission File No. 1823189*

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 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.

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

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[.]”

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]. 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.

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).

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.

Attachment

Declaration of Christopher Ghazarian

Executed on Dec. 20, 2019

DECLARATION OF CHRISTOPHER GHAZARIAN
PURSUANT TO 28 U.S.C. § 1746

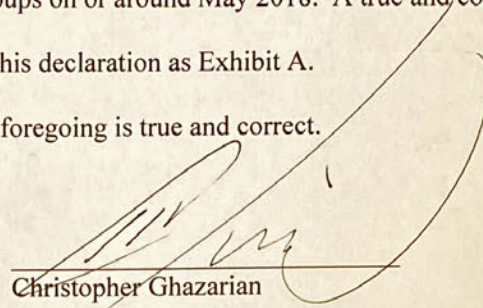
I, Christopher Ghazarian, have personal knowledge of the following facts and matters discussed in this declaration. If called as a witness, I would testify as follows:

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