epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

FEDERAL TRADE COMMISSION

In the Matter of ReadyTech

FTC File No. 1823100

August 1, 2018

By notice published on July 9, 2018, the Federal Trade Commission ("FTC") has proposed a Consent Order with ReadyTech that would settle alleged violations of federal law.[1] The proposed Consent Order would settle alleged "false or misleading" representations that ReadyTech made concerning their compliance with and participation in the E.U.-U.S. Privacy Shield framework.[2]

The Consent Order follows the FTC Complaint, which alleges that ReadyTech, a provider of online training services, deceptively represented that it was actively in the process of certifying compliance with the E.U.-U.S. Privacy Shield framework. In fact, ReadyTech never

---

[1] In the Matter of ReadyTech Corp. (Decision and Order), FTC Dkt. No. 182-3100 (Jul. 2, 2018), https://www.ftc.gov/system/files/documents/cases/1823100_readytech_corp_decision_and_order_7-2-18.pdf [hereinafter Consent Order]; *see also*, Fed. Trade Comm'n., *California Company Settles FTC Charges Related to Privacy Shield Participation*, Press Release, (Jul. 2, 2018), https://www.ftc.gov/news-events/press-releases/2018/07/california-company-settles-ftc-charges-related-privacy-shield.

[2] In the Matter of ReadyTech Corp. (Analysis to Aid Public Comment), FTC Dkt. No. 182-3100, https://www.ftc.gov/system/files/documents/cases/readytech_analysis_7-2-18.pdf; *see also* In the Matter of ReadyTech Corp. (Complaint), FTC Dkt. No. 182-3100 (Jul. 2, 2018), https://www.ftc.gov/system/files/documents/cases/1823100_readytech_complaint_7-2-18.pdf [hereinafter Complaint].

completed the necessary steps to finalize its application and was not certified to participate in the E.U.-U.S. Privacy Shield framework.[3]

Pursuant to this notice, the Electronic Privacy Information Center ("EPIC") submits the following comments to recommend specific changes to the proposed Consent Order, encourage the FTC to uphold the E.U.-U.S. Privacy Shield, and ask the FTC to enforce strong protections for both European and American consumers. The proposed settlement in this matter comes at a critical moment for the continuation of the E.U.-U.S. Privacy Shield. Because of the FTC's inability to sanction companies for failure to comply with Privacy Shield, among other reasons, the European Parliament has called for the suspension of the program, with dire results for the cross-border transfer of data.[4]

EPIC is a public interest research center located in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging civil liberties issues and is a leading consumer advocate before the FTC.[5] EPIC has a particular interest in protecting consumer privacy and has played a leading role in developing the authority of the FTC to address emerging privacy issues and to safeguard the privacy rights of consumers. EPIC has previously filed several complaints with the FTC regarding business practices that harm consumer privacy,[6]

---

[3] *Id.* at ¶ 9-10.

[4] *European Parliament Resolution on the Adequacy of the Protection Afforded by the E.U.-U.S. Privacy Shield*, Eur. Parliament ¶ 12 (Jun. 26, 2018), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+MOTION+B8-2018-0305+0+DOC+PDF+V0//EN, [here after *E.U. Resolution*]

[5] See, e.g., Letter from EPIC Executive Director Marc Rotenberg to FTC Commissioner Christine Varney, EPIC (Dec. 14, 1995) (urging the FTC to investigate the misuse of personal information by the direct marketing industry), http://epic.org/privacy/internet/ftc/ftc_letter.html; EPIC, In the Matter of DoubleClick, (Complaint and Request for Injunction, Request for Investigation and for Other Relief), before the Fed. Trade Comm'n., (Feb. 10, 2000), http://epic.org/privacy/internet/ftc/DCLK_complaint.pdf; EPIC, In the Matter of Microsoft Corporation, (Complaint and Request for Injunction, Request for Investigation and for Other Relief), before the Fed. Trade Comm'n., (Jul. 26, 2001), http://epic.org/privacy/consumer/MS_complaint.pdf; EPIC, In the Matter of Choicepoint, (Request for Investigation and for Other Relief), before the Fed. Trade Comm'n., (Dec. 16, 2004), http://epic.org/privacy/choicepoint/fcraltr12.16.04.html.

[6] *E.g.*, In the Matter of Uber Technologies., Inc. (Complaint, Request for Investigation, Injunction, and Other Relief), (Jun. 22, 2015), https://epic.org/privacy/internet/ftc/uber/Complaint.pdf; In the Matter of Google, Inc. (Complaint, Request for Investigation, Injunction, and Other Relief), (Jul, 31, 2017),

including specific comments on proposed consent orders with other companies who misrepresented their participation in privacy frameworks.[7] EPIC complaints have resulted in substantial investigations[8] and EPIC's comments on proposed settlements have resulted in changes in those orders.[9]

EPIC's comments are divided into four sections. Section I sets out the FTC's legal obligations in considering these comments before finalizing its Consent Order with ReadyTech. Section II underscores the critical role the FTC plays in enforcing Privacy Shield and protecting consumers on both sides of the Atlantic. Section III summarizes the Commission's Complaint and proposed Consent Order. Section IV sets out EPIC's proposed modifications to the Consent Order. In short, the FTC should require ReadyTech to (1) undergo and publicly release independent privacy assessments, (2) disgorge all data collected from E.U. citizens, and (3) implement Fair Information Practices (FIPs).

I. The FTC has a legal obligation to consider public comments prior to finalizing any Consent Order.

The Administrative Procedure Act requires that the Commission take public comments before finalizing any consent order and gives the Commission authority to modify an agreement based on those comments. EPIC has previously submitted several comments to the Commission on preliminary consent orders, subject to public review, that implicate the privacy interests of

---

https://www.epic.org/privacy/ftc/google/EPIC-FTC-Google-Purchase-Tracking-Complaint.pdf; In the Matter of Snapchat, Inc. (Complaint, Request for Investigation, Injunction and Other Relief), (May 16, 2013), https://epic.org/privacy/ftc/EPIC-Snapchat-Complaint.pdf.

[7] *E.g.*, Comments of EPIC, In the Matter of Apperian, Inc., et al, FTC File Nos. 142-3017-3020 et al, (Feb. 20, 2014), https://epic.org/privacy/ftc/EPIC-FTC-Safe-Harbor-Comments.pdf; Comments of EPIC, In the Matter of PayPal Inc., FTC Dkt. No. 162-3102 (Mar. 29, 2016), https://epic.org/apa/comments/EPIC-FTC-PayPal-ConsentOrder.pdf.

[8] *E.g.*, In the Matter of Google, Inc. (Complaint, Request for Investigation, Injunction, and Other Relief), (Feb. 16, 2010), https://epic.org/privacy/ftc/googlebuzz/GoogleBuzz_Complaint.pdf; In the Matter of Facebook, Inc. (Complaint, Request for Investigation, Injunction, and Other Relief), (Dec. 17, 2009), https://epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf.

[9] Comments of EPIC, In the Matter of Uber Technologies, Inc., FTC File No. 152-3054, (Sep. 15, 2017), https://epic.org/apa/comments/EPIC-FTC-Uber-Settlement.pdf.

consumers.[10] Additionally, EPIC has set out recommendations that would have established stronger data protection safeguards for consumers, consistent with the purpose of these settlements. However, the Commission has ordinarily adopted these consent orders without any modification.[11] Nevertheless, EPIC offers these recommendations for the ReadyTech settlement to strengthen the proposed settlement and to encourage more robust enforcement of the E.U.-U.S. Privacy Shield.

These comments set forth why in this settlement, EPIC's proposed modifications arise specifically from ReadyTech's conduct, and are therefore within the FTC's authority. EPIC reminds the Commission that its authority to solicit public comment is pursuant to agency regulations, and the Commission has clear authority to modify a consent order. Commission Rules of Practice, 16 C.F.R. § 2.34 states:

> **(c) Public Comment.** Promptly after its acceptance of the consent agreement, the Commission will place the order contained in the consent agreement, the complaint, and the consent agreement on the public record for a period of 30 days, or such other period as the Commission may specify, for the receipt of comment or views from any interested person.
>
> **(e) Action following comment period.**
> **(2)** The Commission, following the comment period, may determine, on the basis of the comments or otherwise, that a Final Decision and Order that was issued in advance of the comment period should be modified. Absent agreement by respondents to the modifications, the Commission may initiate a proceeding to reopen and modify the decision and order in accordance with § 3.72(b) of this chapter or commence a new administrative proceeding by issuing a complaint in accordance with § 3.11 of this chapter.

[10] *E.g.*, Comments of EPIC, In re Snapchat, Inc., FTC Dkt. No. 132-3078 (Jun. 9, 2014), https://epic.org/apa/comments/FTC-Snapchat-Cmts.pdf; Comments of EPIC, In re Myspace LLC, FTC Dkt. No. 102-3058 (June 8, 2012), https://epic.org/privacy/socialnet/EPIC-Myspace-comments-FINAL.pdf; Comments of EPIC, In re Facebook, Inc., FTC Dkt. No. 092-3184 (Dec. 27, 2011), https://epic.org/privacy/facebook/Facebook-FTC-Settlement-Comments-FINAL.pdf; Comments of EPIC, In re Google, FTC Dkt. No. 102-3136 (May 2, 2011), https://epic.org/privacy/ftc/googlebuzz/EPIC_Comments_to_FTC_Google_Buzz.pdf.

[11] EPIC does note that the Commission modified the Uber Order to require the company to implement additional data security measures and notify the Commission of all future data breaches. *See*, In the Matter of Uber Technologies, Inc. (Decision and Order), FTC File No. 152-3054, (Apr. 12, 2018).

Failure by the Commission to pursue modifications to proposed orders pursuant to public comment would therefore reflect a lack of diligence on the part of the Commission. Even if the Commission decides not to modify the settlement, it must provide a "reasoned response," as it has previously.[12]

II. The enforcement of Privacy Shield requires actual penalties for companies that are not in compliance, and actual remedies for individuals whose rights are violated

According to the FTC, the Privacy Shield satisfies the E.U.'s specific standards for commercial data transfers and allows U.S.-based companies to "transfer data outside the EU consistent with EU law."[13] According to the U.S. Department of Commerce, the Privacy Shield is an exception to a general principle of E.U. law that prohibits data transfers outside of the E.U. where strict E.U. privacy laws do not apply. Joining the Privacy Shield is entirely voluntary for U.S.-based companies.[14] A U.S.-based company that seeks to join the Privacy Shield must complete two steps.[15] First, the company must certify itself to the Department of Commerce. Second, the company must publicly promise to comply with the requirements of the Privacy Shield.[16] Once both steps are completed, a U.S.-based company must comply with Privacy Shield and violations are enforceable under U.S. law.[17]

The FTC plays a pivotal role in enforcing Privacy Shield. It is critical for the FTC to hold accountable those representing that they are complying with Privacy Shield. To date, the FTC

[12] Interstate Nat. Gas Ass'n of Am. v. F.E.R.C., 494 F.3d 1092, 1096 (D.C. Cir. 2007); s*ee also* Response of FTC Secretary Donald S. Clark to EPIC, In re Google Inc., FTC File No. 102-3136, Dkt. No. C-4336 (Oct. 13, 2011), https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzepic.pdf; Letter from Donald Clark, Secretary, Fed. Trade Comm'n. to Marc Rotenberg, Exec. Dir., EPIC, In the Matter of PayPal, Inc. FTC File No. 1623102, Dkt. No. C-4651, (Jul. 23, 2018).
[13] Analysis to Aid Public Comment, *supra* note 2, at 2.
[14] *Fact Sheet: Overview of the EU-U.S. Privacy Shield Framework for Interested Participants*, Dep't of Commerce 1 (Jul. 12, 2016), https://www.commerce.gov/sites/commerce.gov/files/media/files/2016/fact_sheet-_eu-us_privacy_shield_7-16_sc_cmts.pdf.
[15] *Id.*
[16] *Id.*
[17] *Id.*

has brought numerous enforcement proceedings concerning Privacy Shield and its predecessor Safe Harbor. In each case, however, the settlements have failed to provide any redress to E.U. consumers. The European Commission has stated that the availability of redress mechanisms for E.U. citizens is an essential component of Privacy Shield.[18] The FTC's Privacy Shield settlements have merely prohibited companies from making future misrepresentations regarding their participation in Privacy Shield or any other international privacy framework.[19] These settlements are inadequate because they neither provide a remedy to the E.U. consumers whose personal data was wrongfully obtained nor do they require companies to disgorge the data they fraudulently obtained. EPIC highlighted a similar lack of redress in settlements enforcing the Safe Harbor agreement, which was invalidated by the Court of Justice for the European Union in 2015.[20]

The European Parliament recently warned that the FTC's failure to enforce Privacy Shield will result in suspension of the agreement. On June 26, 2018, the E.U. Parliament passed a resolution outlining several problems with the U.S.'s current enforcement of Privacy Shield.[21] The resolution specifically mentioned the Cambridge Analytica breach of 87 million Facebook users' data.[22] Members of the European Parliament (MEPs) expressed concern that data breaches like the Facebook-Cambridge Analytica breach may pose a threat to the democratic process.[23] The resolution emphasized that the FTC needs to more effectively monitor companies under

[18] Eur. Comm'n., *Restoring trust in transatlantic data flows through strong safeguards: European Commission presents EU-U.S. Privacy Shield*, Press Release, (Feb. 29, 2016), http://europa.eu/rapid/press-release_IP-16-433_en.htm.
[19] Fed. Trade Comm'n., *Three Companies Agree to Settle FTC Charges They Falsely Claimed Participation in EU-US Privacy Shield Framework*, Press Release, (Sep. 8, 2017), https://www.ftc.gov/news-events/press-releases/2017/09/three-companies-agree-settle-ftc-charges-they- falsely-claimed.
[20] Comments of EPIC, In the Matter of Apperian, Inc., et al, FTC File Nos. 142-3017-3020 et al, (Feb. 20, 2014), https://epic.org/privacy/ftc/EPIC-FTC-Safe-Harbor-Comments.pdf.
[21] *E.U. Resolution*, *supra*, note 4.
[22] *Id.* at ¶ 9
[23] *Id.* at ¶ 14.

Privacy Shield and, when revelations of data misuse come to light, the FTC must "act upon such revelations without delay" and, if necessary, remove companies that have misused personal data from the Privacy Shield list.[24] The resolution stated that the Facebook-Cambridge Analytica breach "highlight[s] the need for proactive oversight and enforcement actions" that include "systematic checks of the practical compliance of privacy policies … throughout the certification lifecycle."[25] The European Parliament voted to suspend Privacy Shield if the U.S. does not comply with the provisions in full by September 1, 2018.[26]

In addition, the E.U. Parliament's Article 29 Working Party conducted its first annual review of Privacy Shield back in November 2017. MEPs called on the Department of Commerce and the FTC to ensure that self-certified organizations concretely implement the requirements of the Privacy Shield:[27]

> WP29 [hence] believes that it is of utmost importance that the current supervision practice be broadened to routine monitoring by DOC and/or FTC for detecting false claims of participation in the Privacy Shield, in particular through internet searches, as well as to monitor—on an ongoing basis—effective compliance with the Privacy Shield principles by the certified companies.[28]

Because Privacy Shield is a system based on the concept of self-certification, "it is of utmost importance that U.S. authorities involved in the administration of the Privacy Shield devote sufficient resources at oversight and enforcement activities of the certified companies after the actual certification/recertification procedure."[29]

---

[24] *Id*. at ¶ 12.
[25] *Id.* at ¶ 9.
[26] *Id.* at ¶ 35.
[27] *First Annual Joint Review of the E.U.-U.S. Privacy Shield*, Article 29 Data Protection Working Party (Nov. 28, 2017), https://www.lexology.com/library/detail.aspx?g=4f220a3d-69c2-4e9b-bf63-a70aa43b0ee5.
[28] *Id.*
[29] *Id.*

In a related matter, EPIC and consumer privacy organization have urged the FTC to enforce the 2011 Consent Order against Facebook.[30] Because Facebook is certified under Privacy Shield, and also because original Order found that Facebook made false representations about compliance with Safe Harbor,[31] it is vitally important that the FTC make a determination in the Facebook investigation to restore some credibility to the Privacy Shield oversight process.

Without the Privacy Shield, individuals on both sides of the Atlantic will be put at risk and lose trust in the digital economy. The Privacy Shield should be upheld to ensure that there are guardrails around the flow of data from the E.U. to the U.S. and vice versa. Promoting the free flow of personal data across national boundaries requires comprehensive privacy protection. Strengthening the Consent Order with ReadyTech will reassure U.S. trading partners that companies cannot misrepresent their compliance with the Privacy Shield provisions without significant consequences.

III. The Commission has identified significant unfair and deceptive business practices and privacy violations by ReadyTech.

A. Allegations in the Complaint

The FTC Complaint details significant unfair and deceptive trade practices by ReadyTech concerning the privacy of its users.[32] ReadyTech provides online and instructor-led training program to its customers.[33] ReadyTech represented to its users on its website that, "ReadyTech is in the process of certifying that we comply with the U.S. – E.U. Privacy Shield framework as set forth by the U.S. Department of Commerce regarding the collection, use and retention of

[30] *See*, Letter from leading consumer privacy organizations in the United States to Acting Chairman Maureen Ohlhausen and Commissioner Terrell McSweeney (Mar. 20, 2018), https://epic.org/privacy/facebook/EPIC-et-al-ltr-FTC-Cambridge-FB-03-20-18.pdf. *See also*, EPIC, *EPIC, Consumer Groups Urge FTC To Investigate Facebook* (Mar. 20, 2018), https://epic.org/2018/03/epic-consumer-groups-urge-ftc-.html.
[31] *See*, In the Matter of Facebook, Inc. (Decision and Order), FTC File No. 092-3184 (2012), https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf.
[32] Complaint, *supra* note 2.
[33] *Id.* at ¶ 2.

personal data from European Union member countries."[34] Although ReadyTech initiated an application to the Department of Commerce in October 2016 for Privacy Shield certification, the company never completed the steps necessary to participate in Privacy Shield.[35] These acts and practices constitute deceptive acts or practices, in or affecting commerce, in violation of Section 5(a) of the Federal Trade Commission Act.[36]

B. The Commission's Proposed Settlement with ReadyTech

Finding that ReadyTech engaged in false and misleading representations regarding its compliance with the E.U.-U.S. Privacy Shield framework, the Commission has proposed an Order requiring ReadyTech to: (1) not make 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 E.U.-U.S. Privacy Shield framework and the Swiss-U.S. Privacy Shield framework; (2) acknowledge the Order and disseminate the Order now and in the future to persons with responsibilities relating to the subject matter of the Order; (3) notify the FTC of changes in corporate status and mandates that ReadyTech submit an initial compliance report to the FTC; (4) retain documents relating to its compliance with the Order for a five-year period; and (5) make available to the FTC information or subsequent compliance reports, as requested.[37] The Order includes a provision "sunsetting" the Order after twenty years, with certain exceptions.[38]

[34] *Id.* at ¶ 9.
[35] *Id.* at ¶ 10.
[36] *Id.* at ¶ 13.
[37] Consent Order, *supra* note 1.
[38] Analysis to Aid Public Comment, *supra* note 2, at 2.

IV. The Consent Order should be modified to require that ReadyTech release independent privacy assessments to the public, disgorge data unlawfully collected from E.U. citizens, and implement the Fair Information Practices.

EPIC supports the finding of the Commission and the proposed Order. The Order will prohibit ReadyTech from engaging in misrepresentations that lead consumers to believe that their information is being protected consistent with the E.U.-U.S. Privacy Shield requirements. However, the proposed Consent Order is still insufficient to adequately protect the privacy and security of ReadyTech users. EPIC urges the Commission to make the following modifications.

A. The FTC Consent Order should require ReadyTech to undergo and publicly release independent privacy assessments.

The FTC should amend the proposed Consent Order to require ReadyTech to undergo independent privacy assessments on a biennial basis. In addition to the required compliance reports, these independent audits will ensure that ReadyTech maintains adequate privacy protections for its users and will help determine if they are in compliance with Privacy Shield requirements. These assessments should "be completed by a qualified, objective, independent third-party professional" and occur every two years for the next 5 to 10 years, similar to the FTC's Consent Order with Paypal/Venmo.[39] Each assessment must (1) detail specific privacy controls ReadyTech has put in place; (2) explain how the privacy controls are appropriate given ReadyTech's size, nature and scope of their activities, and sensitivity of the information being stored; (3) explain how the privacy controls being used meet or exceed the provisions of the Consent Order; and (4) certify that privacy controls are operating effectively and provide reasonable assurances that the privacy of consumer information will be protected.

[39] In the Matter of PayPal, Inc. (Decision and Order), FTC, Dkt. No. 162-3102 (Mar. 5, 2018), https://www.ftc.gov/system/files/documents/cases/venmo_agreement_with_decision.pdf.

Additionally, the FTC should modify the proposed Consent Order to require that ReadyTech release its privacy assessments to the public. Releasing required privacy assessments will help the public determine whether they can safely and securely continue to use ReadyTech's services. Required independent privacy assessments are a good step to ensure that ReadyTech takes concrete steps to reform its consumer data and privacy practices. However, in an effort to restore public trust in ReadyTech's services and the E.U.-U.S. Privacy Shield framework as a whole, the FTC should require that all assessments be made available to the public. This trust is particularly essential given the FTC's recent failure to enforce the 2011 Facebook Consent Order, resulting in the unlawful transfer of 87 million user records to Cambridge Analytica.[40] Releasing ReadyTech's privacy assessments will signal that the FTC is not abdicating its enforcement authority and duty to protect the public.

Crucially, publicly available assessments will also assure both American and European consumers that ReadyTech has adequate privacy measures in place. In its resolution to suspend Privacy Shield because of lack of adequate privacy protection in the U.S., the European Parliament called for "proactive oversight and enforcement actions . . . which include *systematic checks of the practical compliance* of privacy policies with the Privacy Shield principles throughout the certification lifecycle" (emphasis added).[41] To ensure adequacy and in turn compliance with Privacy Shield, therefore, it is incumbent on the FTC to enforce "systematic checks" such as the proposed publicly available privacy assessments. These checks will provide a robust monitoring mechanism where public participation can both ease the FTC's regulatory burden and ensure Privacy Shield compliance.

[40] Marc Rotenberg, *How the FTC Could Have Prevented the Facebook Mess*, Techonomy (Mar. 22, 2018), https://techonomy.com/2018/03/how-the-ftc-could-have-avoided-the-facebook-mess.
[41] *E.U. Resolution*, *supra* note 4, at ¶ 9.

In response to EPIC's comments in *In the Matter of PayPal, Inc.*, which similarly proposed releasing privacy assessment to the public, the FTC Secretary wrote that "the public may seek access to compliance reports by requesting them under the Freedom of Information Act."[42] Putting the burden of requesting information on the public, however, essentially denies ordinary consumers the right to access crucial privacy reports. Submitting FOIA requests is a time-consuming and burdensome process that requires special knowledge of the legal process. It is mostly done by organizations with expertise in the area such as EPIC. Ordinary consumers cannot realistically be expected to possess this expertise and submit FOIA requests on their own. Therefore, the burden should therefore be on the companies and the FTC to release privacy assessments. Furthermore, the FTC has already publicly released privacy assessments for many companies under Consent Order,[43] and it should not present any special difficulty for the Commission to publicly release all privacy assessments to inform the public about the privacy protections they receive.

B. The FTC should require ReadyTech to disgorge data collected from E.U. citizens.

The FTC should modify the Consent Order to require that ReadyTech disgorge all data collected from E.U. citizens. Given ReadyTech's failure to comply with Privacy Shield requirements, data collected from E.U. citizens was collected illegally. Users should be alerted to this illegal collection and their data should be returned to them. Furthermore, all illegally collected data should be deleted from ReadyTech servers to avoid data abuse and unfair benefit

[42] *Letters to Commenters*, In the Matter of PayPal, Inc., FTC File No. 1623102, Dkt. No. C-4651, at 19-20 (Jul. 23, 2018), https://www.ftc.gov/system/files/documents/cases/venmo_letters_to_commenters_5-24-18.pdf [hereinafter PayPal Response].
[43] *Id.* at 20.

to ReadyTech.[44] Only when ReadyTech is complying with E.U.-U.S. Privacy Shield requirements should the company be permitted to resume collecting data from E.U. citizens.

C. ReadyTech should be required to implement Fair Information Practices (FIPs).

Implementation of the FIPs directly addresses the conduct at issue by ReadyTech, and it is critical that the FTC set up affirmative requirements for a company to comply with Privacy Shield. The FTC should modify the Consent Order to require that ReadyTech implement FIPs, an internationally accepted privacy framework. The Code of Fair Information Practices sets out responsibilities in the collection and use of personal data, and therefore will assist in ensuring compliance with Privacy Shield requirements.[45] It serves as the starting point for modern privacy law and was incorporated into the Privacy Act of 1974.[46] The FIPs are also found in other privacy laws and frameworks, such as the Organization for Economic Cooperation and Development ("OECD") Privacy Guidelines[47] and the European Commission's General Data Protection Regulation ("GDPR").[48] This common approach to privacy protection therefore helps enable international data transfer consistent with the goals of Privacy Shield.

Importantly, implementing FIPs can help ReadyTech comply with the Privacy Shield framework. Under the FIPs, a company must (1) not have secret personal data record-keeping systems; (2) allow users to access the information stored about them and know how it is used; (3) not use personal data obtained for one purpose for a different purpose without consent; (4) allow

---

[44] The Commission has previously imposed this requirement in consumer privacy settlements. *See*, In the Matter of Goldenshores Technologies, LLC, (Decision and Order) FTC File No. 132-3087 (2014), https://www.ftc.gov/system/files/documents/cases/140409goldenshoresdo.pdf.

[45] EPIC, *The Code of Fair Information Practices*, https://epic.org/privacy/consumer/code_fair_info.html.

[46] *See* Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy*, 2001 Stan. Tech. L. Rev. 1.

[47] *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Org. Econ. Coop. & Dev., http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

[48] *Proposal for a Regulation of the European Parliament and the Council on the Protection of Individuals with regard to the Processing of Personal Data and the Free Movement of Such Data (General Data Protection Regulation)*, Eur. Comm'n (Jan. 25, 2012), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0011&from=EN.

users to correct errors in identifiable information kept about them; and (5) assure the reliability of the data for their intended use and take precautions to prevent misuse of personal data.[49] These practices reflect "a set of principles and related requirements that have been deemed by the European Commission as providing 'adequate' privacy protection" and which are required for Privacy Shield compliance, including "notice; choice; accountability for onward transfer; security; data integrity and purpose limitation; access; and recourse, enforcement, and liability."[50] Specifically, the first FIP prevents secret data collection and thus helps satisfy the notice requirement; the second aids both access and notice; the third is consistent with purpose limitation; the fourth serves the recourse requirement; and the fifth promotes data integrity and security.

In response to EPIC's comments in *In the Matter of PayPal, Inc.*, the FTC Secretary wrote that "a settlement agreement is designed to address specific conduct alleged in a complaint and may not impose additional obligations that are not reasonably related to such conduct or preventing its recurrence."[51] In the *PayPal* case, the challenged conduct related to misrepresentations about fund availability for bank transfer, privacy of transactions, and user account security. Here, however, ReadyTech's challenged conduct is its misrepresentation of compliance with Privacy Shield. Implementing FIPs would ensure such compliance because, as explained above, the FIPs provide privacy protections that satisfy the requirements of Privacy Shield. Implementation of the FIPs is therefore reasonably related to ReadyTech's challenged conduct and preventing its recurrence. Furthermore, the FIPs are technology-neutral

[49] EPIC, *The Code of Fair Information Practices*, https://epic.org/privacy/consumer/code_fair_info.html.
[50] Analysis to Aid Public Comment, *supra* note 2, at 1; *see also Privacy Shield Framework*, Int'l Trade Admin., U.S. Dep't of Commerce, https://www.privacyshield.gov/E.U.-US-Framework (setting out the specific provisions under these elements).
[51] PayPal Response, *supra* note 31, at 19.

requirements and will thus increase the longevity of the Consent Order by ensuring it remains relevant to ReadyTech's business practices over the course of the 20 years it will be in effect.

V. Conclusion

EPIC supports the findings of the FTC concerning ReadyTech's false and misleading representations of its participation in Privacy Shield. But the FTC must do more to enforce Privacy Shield and safeguard the free flow of data between the United States and Europe. Specifically, EPIC urges the FTC to require ReadyTech to undergo and publicly release independent privacy assessments, disgorge all data collected from E.U. citizens, and implement Fair Information Practices.

The FTC is under a legal obligation to consider these comments before finalizing the Order with ReadyTech and must provide a reasoned response if it fails to modify the Order as described above. EPIC urges the Commission to adopt the changes to the proposed Consent Order set out above.

Respectfully submitted,

/s/ *Marc Rotenberg*
Marc Rotenberg
EPIC President

/s/ *Christine Bannan*
Christine Bannan
EPIC Administrative Law Fellow

/s/ *Sam Lester*
Sam Lester
EPIC Consumer Privacy Fellow

/s/ *Allison Gilley*
Allison Gilley
EPIC Law Clerk

/s/ *Nicole Sakin*
Nicole Sakin
EPIC Law Clerk

/s/ *Shili Shao*
Shili Shao
EPIC Law Clerk