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

Office of the Chair

July 13, 2023

The Right Honorable Chloe Smith MP
Secretary of State
Department of Science, Innovation
and Technology (DSIT)
100 Parliament Street
London
United Kingdom
SW1A 2BQ

Dear Secretary of State Smith:

The United States Federal Trade Commission ("FTC") appreciates the opportunity to address its enforcement role in connection with the EU-U.S. Data Privacy Framework ("EU-U.S. DPF") Principles as relates to personal data transfers from the United Kingdom. The FTC has long committed to protecting consumers and privacy across borders, and we are committed to enforcement of the commercial sector aspects of this framework. The FTC has performed such a role since the year 2000, in connection with the U.S.-EU Safe Harbor Framework, and most recently since 2016, in connection with the EU-U.S. Privacy Shield Framework.[1] On July 16, 2020, the Court of Justice of the European Union ("CJEU") invalidated the European Commission's adequacy decision underlying the EU-U.S. Privacy Shield Framework, on the basis of issues other than the commercial principles that the FTC enforced. The U.S. and the European Commission have since negotiated the EU-U.S. Data Privacy Framework to address that CJEU ruling, and relatedly the United States and the UK Government have since negotiated the United Kingdom Extension to the EU-U.S. Data Privacy Framework ("UK Extension to the EU-U.S. DPF").

I write to confirm the FTC's commitment to vigorous enforcement of the EU-U.S. DPF Principles under the UK Extension to the EU-U.S. DPF. Notably, we affirm our commitment in

[1] Letter from Chairwoman Edith Ramirez to Věra Jourová, Commissioner for Justice, Consumers and Gender Equality of the European Commission, Describing Federal Trade Commission Enforcement of the New EU-U.S. Privacy Shield Framework (Feb. 29, 2016), https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/letter-chairwoman-edith-ramirez-vera-jourova-commissioner-justice-consumers-gender-equality-european. The FTC also previously committed to enforce the U.S-EU Safe Harbor Program. Letter from Robert Pitofsky, FTC Chairman, to John Mogg, Director DG Internal Market, European Commission (July 14, 2000), https://www.federalregister.gov/documents/2000/07/24/00-18489/issuance-of-safe-harbor-principles-and-transmission-to-european-commission. This letter replaces those earlier commitments as relates to personal data transfers from the United Kingdom and Gibraltar.

three key areas: (1) referral prioritization and investigations; (2) seeking and monitoring orders; and (3) enforcement cooperation with the UK Information Commissioner's Office ("ICO").[2]

I. Introduction

a. FTC Privacy Enforcement and Policy Work

The FTC has broad civil enforcement authority to promote consumer protection and competition in the commercial sphere. As part of its consumer protection mandate, the FTC enforces a wide range of laws to protect the privacy and security of consumers and their data. The primary law enforced by the FTC, the FTC Act, prohibits "unfair" or "deceptive" acts or practices in or affecting commerce.[3] The FTC also enforces targeted statutes that protect information relating to health, credit, and other financial matters, as well as children's online information, and has issued regulations implementing each of these statutes.[4]

The FTC has also recently pursued numerous initiatives to strengthen our privacy work. In August of 2022 the FTC announced it is considering rules to crack down on harmful commercial surveillance and lax data security.[5] The goal of the project is to build a robust public record to inform whether the FTC should issue rules to address commercial surveillance and data security practices, and what those rules should potentially look like.

Our "PrivacyCon" conferences continue to gather leading researchers to discuss the latest research and trends related to consumer privacy and data security. We also have increased our agency's ability to keep pace with the technology developments at the center of much of our privacy work, building a growing team of technologists and interdisciplinary researchers. In 2014 the FTC and the ICO signed a Memorandum of Understanding, and we have cooperated in numerous public and non-public matters since.[6] We also recently issued a report to Congress warning about harms associated with using artificial intelligence ("AI") to address online harms

---

[2] The Gibraltar Regulatory Authority ("GRA") as relates to personal data transfers from Gibraltar.

[3] 15 U.S.C. § 45(a). The FTC does not have jurisdiction over criminal law enforcement or national security matters. Nor can the FTC reach most other governmental actions. In addition, there are exceptions to the FTC's jurisdiction over commercial activities, including with respect to banks, airlines, the business of insurance, and the common carrier activities of telecommunications service providers. The FTC also does not have jurisdiction over most non-profit organizations, though it does have jurisdiction over sham charities or other non-profits that in fact operate for profit. The FTC also has jurisdiction over non-profit organizations that operate for the profit of their for-profit members, including by providing substantial economic benefits to those members. In some instances, the FTC's jurisdiction is concurrent with that of other law enforcement agencies. We have developed strong working relationships with federal and state authorities, and work closely with them to coordinate investigations or make referrals where appropriate.

[4] *See* Privacy and Security, https://www.ftc.gov/business-guidance/privacy-security.

[5] *See* Press Release, Fed. Trade Comm'n, FTC Explores Rules Cracking Down on Commercial Surveillance and Lax Data Security Practices (Aug. 11, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-explores-rules-cracking-down-commercial-surveillance-lax-data-security-practices.

[6] *See* Press Release, Fed. Trade Comm'n, FTC Signs Memorandum of Understanding with UK Privacy Enforcement Agency (Mar. 6, 2014), https://www.ftc.gov/news-events/news/press-releases/2014/03/ftc-signs-memorandum-understanding-uk-privacy-enforcement-agency.

identified by Congress. This report raised concerns regarding inaccuracy, bias, discrimination, and commercial surveillance creep.[7]

b. U.S. Legal Protections Benefitting UK Consumers

The UK Extension to the EU-U.S. DPF operates in the context of the larger U.S. privacy landscape, which also protects UK consumers in a number of ways. The FTC Act's prohibition on unfair or deceptive acts or practices is not limited to protecting U.S. consumers from U.S. companies, as it includes those practices that (1) cause or are likely to cause reasonably foreseeable injury in the United States, or (2) involve material conduct in the United States. Further, the FTC can use all remedies that are available to protect domestic consumers when protecting foreign consumers.[8]

The FTC also enforces other targeted laws whose protections extend to non-U.S. consumers, such as the Children's Online Privacy Protection Act ("COPPA"). Among other things, COPPA requires that operators of child-directed websites and online services, or general audience sites that knowingly collect personal information from children under the age of 13, provide parental notice and obtain verifiable parental consent. U.S.-based websites and services that are subject to COPPA and collect personal information from foreign children are required to comply with COPPA. Foreign-based websites and online services must also comply with COPPA if they are directed to children in the United States, or if they knowingly collect personal information from children in the United States. Moreover, in addition to the U.S. federal laws enforced by the FTC, other federal and state consumer protection, data breach, and privacy laws may provide additional benefits to UK consumers.

c. FTC Enforcement Activity

The FTC brought cases under both the U.S.-EU Safe Harbor and EU-U.S. Privacy Shield frameworks and continued to enforce the EU-U.S. Privacy Shield even after the CJEU invalidation of the adequacy decision underlying the EU-U.S. Privacy Shield Framework.[9] Several of the FTC's recent complaints have included counts alleging that firms violated EU-U.S. Privacy Shield provisions, including in proceedings against Twitter,[10] CafePress,[11] and

---

[7] *See* Press Release, Fed. Trade Comm'n, FTC Report Warns About Using Artificial Intelligence to Combat Online Problems (June 16, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/06/ftc-report-warns-about-using-artificial-intelligence-combat-online-problems.

[8] 15 U.S.C. § 45(a)(4)(B). Further, "unfair or deceptive acts or practices" includes such acts or practices involving foreign commerce that (i) cause or are likely to cause reasonably foreseeable injury within the United States; or (ii) involve material conduct occurring within the United States. 15 U.S.C. § 45(a)(4)(A).

[9] *See* Appendix A for a list of FTC Safe Harbor and Privacy Shield matters.

[10] *See* Press Release, Fed. Trade Comm'n, FTC Charges Twitter with Deceptively Using Account Security Data to Sell Targeted Ads (May 25, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-charges-twitter-deceptively-using-account-security-data-sell-targeted-ads.

[11] *See* Press Release, Fed. Trade Comm'n, FTC Takes Action Against CafePress for Data Breach Cover Up (Mar., 2022), https://www.ftc.gov/news-events/news/press-releases/2022/03/ftc-takes-action-against-cafepress-data-breach-cover.

Flo.[12] In the enforcement action against Twitter, the FTC secured $150 million from Twitter for its violation of an earlier FTC order with practices affecting more than 140 million customers, including violating EU-U.S. Privacy Shield Principle 5 (Data Integrity and Purpose Limitation). Further, the agency's order requires that Twitter allow users to employ secure multi-factor authentication methods that do not require users to provide their telephone numbers.

In *CafePress*, the FTC alleged that the company failed to secure consumers' sensitive information, covered up a major data breach, and violated EU-U.S. Privacy Shield Principles 2 (Choice), 4 (Security), and 6 (Access). The FTC's order requires the company to replace inadequate authentication measures with multifactor authentication, substantively limit the amount of data it collects and retains, encrypt Social Security numbers, and have a third party assess its information security programs and provide the FTC with a copy that can be publicized.

In *Flo*, the FTC alleged that the fertility-tracking app disclosed user health information to third-party data analytics providers after commitments to keep such information private. The FTC complaint specifically notes the company's interactions with EU consumers and that Flo violated EU-U.S. Privacy Shield Principles 1 (Notice), 2 (Choice), 3 (Accountability for Onward Transfer), and 5 (Data Integrity and Purpose Limitation). Among other things, the agency's order requires Flo to notify affected users about the disclosure of their personal information and to instruct any third party that received users' health information to destroy that data. Importantly, FTC orders protect all consumers worldwide who interact with a U.S. business, not just those consumers who have lodged complaints.

Many past U.S.-EU Safe Harbor and EU-U.S. Privacy Shield enforcement cases involved organizations that completed an initial self-certification through the Department of Commerce, but failed to maintain their annual self-certification while they continued to represent themselves as current participants. Other cases involved false claims of participation by organizations that never completed an initial self-certification through the Department of Commerce. Going forward, we expect to focus our proactive enforcement efforts on the types of substantive violations of the EU-U.S. DPF Principles alleged in cases such as Twitter, CafePress, and Flo. Meanwhile, the Department of Commerce will administer and supervise the self-certification process, maintain the authoritative list of EU-U.S. DPF and, as applicable, UK Extension to the EU-U.S. DPF participants, and address other program participation claim issues.[13] Importantly, organizations claiming EU-U.S. DPF and, as applicable, UK Extension to the EU-U.S. DPF participation may be subject to substantive enforcement of the EU-U.S. DPF Principles even if they fail to make or maintain their self-certification through the Department of Commerce.

II. Referral Prioritization and Investigations

[12] *See* Press Release, Fed. Trade Comm'n, FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google, and Others (June 22, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google.

[13] Letter from Marisa Lago, Under Secretary of Commerce for International Trade, to the Right Honorable Chloe Smith MP, Secretary of State, Department of Science, Innovation and Technology (DSIT) (July 13, 2023).

As we did under the U.S.-EU Safe Harbor Framework and the EU-U.S. Privacy Shield Framework, the FTC commits to give priority consideration to EU-U.S. DPF Principles referrals from the Department of Commerce, EU data protection authorities ("DPAs"), and the ICO. We will also prioritize consideration of referrals for non-compliance with the EU-U.S. DPF Principles from privacy self-regulatory organizations and other independent dispute resolution bodies.

To facilitate referrals under the UK Extension to the EU-U.S. DPF from the ICO, the FTC has created a standardized referral process and has provided guidance to the ICO on the type of information that would best assist the FTC in its inquiry into a referral. As part of this effort, the FTC has designated an agency point of contact for ICO referrals. It is most useful when the ICO has conducted a preliminary inquiry into the alleged violation and can cooperate with the FTC in an investigation.

Upon receipt of such a referral from the Department of Commerce, the ICO, or self-regulatory organization or other independent dispute resolution bodies the FTC can take a range of actions to address the issues raised. For example, we may review the organization's privacy policies, obtain further information directly from the organization or from third parties, follow up with the referring entity, assess whether there is a pattern of violations or significant number of consumers affected, determine whether the referral implicates issues within the purview of the Department of Commerce, assess whether additional efforts to put market participants on notice would be helpful, and, as appropriate, initiate an enforcement proceeding.

In addition to prioritizing EU-U.S. DPF Principles referrals from the Department of Commerce, the ICO, and privacy self-regulatory organizations or other independent dispute resolution bodies,[14] the FTC will continue to investigate significant EU-U.S. DPF Principles violations on its own initiative where appropriate, using a range of tools. As part of the FTC's program of investigating privacy and security issues involving commercial organizations, the agency has routinely examined whether the entity at issue was making EU-U.S. Privacy Shield representations. If the entity made such representations and the investigation revealed apparent violations of the EU-U.S. Privacy Shield Principles, the FTC included allegations of EU-U.S. Privacy Shield violations in its enforcement actions. We will continue this proactive approach, now with respect to the EU-U.S. DPF Principles.

III. Seeking and Monitoring Orders

The FTC also affirms its commitment to seek and monitor enforcement orders to ensure compliance with the EU-U.S. DPF Principles. We will require compliance with the EU-U.S. DPF Principles through a variety of appropriate injunctive provisions in future FTC EU-U.S. DPF Principles orders. Violations of the FTC's administrative orders can lead to civil penalties

[14] Although the FTC does not resolve or mediate individual consumer complaints, the FTC affirms that it will prioritize EU-U.S. DPF Principles referrals from the ICO. In addition, the FTC uses complaints in its Consumer Sentinel database, which is accessible by many other law enforcement agencies, to identify trends, determine enforcement priorities, and identify potential investigative targets. UK individuals can use the same complaint system available to U.S. consumers to submit a complaint to the FTC at https://reportfraud.ftc.gov/. For individual EU-U.S. DPF Principles complaints, however, it may be most useful for UK individuals to submit complaints to the ICO and/or, as applicable, the GRA or independent dispute resolution body.

of up to $ 50,120 per violation, or $50,120 per day for a continuing violation,[15] which, in the case of practices affecting many consumers, can amount to millions of dollars. Each consent order also has reporting and compliance provisions. The entities under order must retain documents demonstrating their compliance for a specified number of years. The orders must also be disseminated to employees responsible for ensuring order compliance.

The FTC systematically monitors compliance with existing EU-U.S. Privacy Shield Principles orders, as it does with all of its orders, and brings actions to enforce them when necessary.[16] Importantly, FTC orders will continue to protect all consumers worldwide who interact with a business, not just those consumers who have lodged complaints. Finally, the FTC will maintain an online list of companies subject to orders obtained in connection with enforcement of the EU-U.S. DPF Principles.[17]

IV. Enforcement Cooperation with the ICO

The FTC recognizes the important role that the ICO can play with respect to EU-U.S. DPF Principles compliance and encourages increased consultation and enforcement cooperation. Indeed, a coordinated approach to the challenges posed by current digital market developments, and data-intensive business models, is increasingly critical. The FTC will exchange information on referrals with referring enforcement authorities, including the status of referrals, subject to confidentiality laws and restrictions. To the extent feasible given the number and type of referrals received, the information provided will include an evaluation of the referred matters, including a description of significant issues raised and any action taken to address law violations within the jurisdiction of the FTC. The FTC will also provide feedback to the referring authority on the types of referrals received in order to increase the effectiveness of efforts to address unlawful conduct. If a referring enforcement authority seeks information about the status of a particular referral for purposes of pursuing its own enforcement proceeding, the FTC will respond, taking into account the number of referrals under consideration and subject to confidentiality and other legal requirements.

The FTC will also work closely with the ICO to provide enforcement assistance. In appropriate cases, this could include information sharing and investigative assistance pursuant to the U.S. SAFE WEB Act, which authorizes FTC assistance to foreign law enforcement agencies when the foreign agency is enforcing laws prohibiting practices that are substantially similar to those prohibited by laws the FTC enforces.[18] As part of this assistance, the FTC can share information obtained in connection with an FTC investigation, issue compulsory process on

[15] 15 U.S.C. § 45(m); 16 C.F.R. § 1.98. This amount is periodically adjusted for inflation.
[16] Last year the FTC voted to streamline the process for investigating repeat offenders. *See* Press Release, Fed. Trade Comm'n, FTC Authorizes Investigations into Key Enforcement Priorities (Jul. 1, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/07/ftc-authorizes-investigations-key-enforcement-priorities.
[17] *Cf.* Privacy Shield, https://www.ftc.gov/business-guidance/privacy-security/privacy-shield.
[18] In determining whether to exercise its U.S. SAFE WEB Act authority, the FTC considers, inter alia: "(A) whether the requesting agency has agreed to provide or will provide reciprocal assistance to the Commission; (B) whether compliance with the request would prejudice the public interest of the United States; and (C) whether the requesting agency's investigation or enforcement proceeding concerns acts or practices that cause or are likely to cause injury to a significant number of persons." 15 U.S.C. § 46(j)(3). This authority does not apply to enforcement of competition laws.

behalf of the ICO conducting its own investigation, and seek oral testimony from witnesses or defendants in connection with the ICO's enforcement proceeding, subject to the requirements of the U.S. SAFE WEB Act. The FTC regularly uses this authority to assist other authorities around the world in privacy and consumer protection cases.

In addition to any consultation with the ICO on case-specific matters, the FTC will participate in periodic meetings with the ICO to discuss in general terms how to improve enforcement cooperation. The FTC will also participate, along with the Department of Commerce, DSIT, and ICO and GRA representatives, as appropriate, in periodic discussions on the UK Extension to the EU-U.S. DPF to discuss its implementation. The FTC also encourages the development of tools that will enhance enforcement cooperation with the ICO, as well as other privacy enforcement authorities around the world. The FTC is pleased to affirm its commitment to enforcing the commercial sector aspects of the UK Extension to the EU-U.S. DPF. We see our partnership with UK colleagues as a critical part of providing privacy protection for both our citizens and yours.

Sincerely,

Lina M. Khan
Chair, Federal Trade Commission