United States of America
FEDERAL TRADE COMMISSION
WASHINGTON, DC 20580

OFFICE OF CHAIRWOMAN
EDITH RAMIREZ

January 9, 2017

VIA EMAIL

Federal Councillor
Johann N. Schneider-Ammann
Head of the Department of Economic Affairs, Education and Research
Bundeshaus Ost
3003 Bern
Switzerland

Dear Federal Councillor:

I appreciate this opportunity to affirm the Federal Trade Commission's commitment to enforce the Swiss-U.S. Privacy Shield Framework, which is modeled on the EU-US Privacy Shield Framework and replaces the U.S.-Swiss Safe Harbor Framework. We believe this new Framework will facilitate continued trade between the United States and Switzerland and strengthen privacy protections for Swiss consumers.

I have previously explained the FTC's commitment to enforce the EU-U.S. Privacy Shield in correspondence to Věra Jourová, the European Union's Commissioner for Justice, Consumers and Gender Equality,[1] and extend these same assurances in connection with the Swiss-U.S. Privacy Shield Framework. In particular, I want to highlight the FTC's commitment in four key areas: (1) referral prioritization and investigations; (2) addressing false or deceptive Privacy Shield membership claims; (3) continued order monitoring; and (4) enhanced engagement and enforcement cooperation. We provide below detailed information about each of these, together with relevant background about the FTC's role in protecting consumer privacy and enforcing the Safe Harbor programs.[2]

---

[1] *See* Letter from Edith Ramirez, Chairwoman, Fed. Trade Comm'n, to Věra Jourová, Commissioner for Justice, Consumers and Gender Equality of the European Commission (July 7, 2016), *available at* https://www.ftc.gov/public-statements/2016/07/letter-chairwoman-edith-ramirez-vera-jourova-commissioner-justice [hereinafter FTC EU-U.S. Privacy Shield Letter].

[2] Additional information about FTC privacy enforcement and policy work and U.S. federal and state privacy laws is provided in the FTC EU-U.S. Privacy Shield Letter, including in Attachment A. In addition, a summary of our recent privacy and security enforcement actions is available on the FTC's website at https://www.ftc.gov/reports/privacy-data-security-update-2015.

I. Background

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 consumer data. The primary law enforced by the FTC, the FTC Act, prohibits "unfair" and "deceptive" acts or practices in or affecting commerce.[3] A representation, omission, or practice is deceptive if it is material and likely to mislead consumers acting reasonably under the circumstances.[4] An act or practice is unfair if it causes, or is likely to cause, substantial injury that is not reasonably avoidable by consumers or outweighed by countervailing benefits to consumers or competition.[5] 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.

The FTC's jurisdiction under the FTC Act applies to matters "in or affecting commerce." 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.[6] The FTC also does not have jurisdiction over most non-profit organizations, but it does have jurisdiction over sham charities or other non-profits that in actuality 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.[7] 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.

Enforcement is the lynchpin of the FTC's approach to privacy protection. To date, the FTC has brought over 500 cases protecting the privacy and security of consumer information. This body of cases covers both offline and online information and includes enforcement actions against companies large and small, alleging that they failed to properly dispose of sensitive consumer data, failed to secure consumers' personal information, deceptively tracked consumers online, spammed consumers, installed spyware or other malware on consumers' computers, violated Do Not Call and other telemarketing rules, and improperly collected and shared consumer information on mobile devices. The FTC's enforcement actions – in both the physical

[3] 15 U.S.C. § 45(a).
[4] *See* FTC Policy Statement on Deception, *appended to Cliffdale Assocs., Inc.*, 103 F.T.C. 110, 174 (1984), *available at* https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception.
[5] *See* 15 U.S.C § 45(n); FTC Policy Statement on Unfairness, *appended to Int'l Harvester Co.*, 104 F.T.C. 949, 1070 (1984), *available at* https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness.
[6] The FTC's longstanding view is that it has jurisdiction over the non-common carrier activities of common carriers. This issue is currently being litigated.
[7] *See California Dental Ass'n v. FTC*, 526 U.S. 756 (1999).

and digital worlds – send an important message to companies about the need to protect consumer privacy.

Our enforcement actions also have a global impact. 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, including restitution, that are available to protect domestic consumers when protecting foreign consumers.

Our cases enforcing Section 5 of the FTC Act have protected the privacy of U.S. and foreign consumers alike. For example, in a case against an information broker, Accusearch, the FTC alleged that the company's sale of confidential telephone records to third parties without consumers' knowledge or consent was an unfair practice in violation of Section 5 of the FTC Act. Accusearch sold information relating to both U.S. and foreign consumers.[8] The court granted injunctive relief against Accusearch prohibiting, among other things, the marketing or sale of consumers' personal information without written consent, unless it was lawfully obtained from publicly available information, and ordered disgorgement of almost $200,000.[9]

Another notable case is our recent action against the Canadian operators of the dating website AshleyMadison.com, in which we alleged, among other things, that the site operators failed to take reasonable steps to secure their users' personal information, resulting in the unauthorized disclosure of sensitive information about 36 million consumers worldwide.[10] This case not only demonstrates the FTC's authority to take action to address cross-border privacy and security law violations but also highlights how effective cooperation with foreign privacy authorities enhances our ability to protect consumers from harmful privacy and security practices that have global implications. Our cooperation with the Canadian and Australian privacy authorities in this case helped us obtain more comprehensive information and investigate the security practices more efficiently, as well as facilitated our collective efforts to protect consumers in countries around the world.

In addition to its enforcement work, the FTC has also pursued numerous policy initiatives aimed at enhancing consumer privacy. The FTC has hosted workshops and issued reports recommending best practices aimed at improving privacy in the mobile ecosystem; increasing transparency of the data broker industry; maximizing the benefits of big data while mitigating its risks, particularly for low-income and underserved consumers; and highlighting the privacy and security implications of facial recognition and the Internet of Things, among other areas. Most recently, the FTC's Fall Technology Series has examined the privacy and security implications of ransomware, drones, and smart entertainment devices.

---

[8] *See* Office of the Privacy Commissioner of Canada, Complaint under PIPEDA against Accusearch, Inc., doing business as Abika.com, https://www.priv.gc.ca/cf-dc/2009/2009_009_0731_e.asp. The Office of the Privacy Commissioner of Canada filed an *amicus curiae* brief in the appeal of the FTC action and conducted its own investigation, concluding that Accusearch's practices also violated Canadian law.

[9] *See FTC v. Accusearch, Inc.*, No. 06CV015D (D. Wyo. Dec. 20, 2007), *aff'd* 570 F.3d 1187 (10th Cir. 2009).

[10] *See FTC v. Ruby Corp.*, No. 1:16-cv-02438 (D.D.C. Dec. 14, 2016).

B. Safe Harbor Enforcement

As part of its robust privacy and security enforcement program, the FTC has sought to protect Swiss and EU consumers by bringing enforcement actions that involved Safe Harbor violations. The FTC has brought 39 Safe Harbor enforcement actions: 36 alleging false certification claims, and three cases—against Google, Facebook, and Myspace—involving alleged violations of Safe Harbor Privacy Principles.[11] Ten of these cases involved the U.S.-Swiss Safe Harbor.[12] These cases demonstrate the enforceability of certifications and the repercussions for non-compliance. Twenty-year consent orders require Google, Facebook, and Myspace to implement comprehensive privacy programs that must be reasonably designed to address privacy risks related to the development and management of new and existing products and services and to protect the privacy and confidentiality of personal information. The comprehensive privacy programs mandated under these orders must identify foreseeable material risks and have controls to address those risks. The companies must also submit to ongoing, independent assessments of their privacy programs, which must be provided to the FTC. The orders also prohibit these companies from misrepresenting their privacy practices and their participation in any privacy or security program. This prohibition would also apply to companies' acts and practices under the new EU-U.S. and Swiss-U.S. Privacy Shield Frameworks. The FTC can enforce these orders by seeking civil penalties. In fact, Google paid a record $22.5 million civil penalty in 2012 to resolve allegations it had violated its order. Consequently, these FTC orders help protect over a billion consumers worldwide, hundreds of millions of whom reside in Europe.

Many of our other Safe Harbor enforcement cases involved organizations that joined the Safe Harbor program but failed to renew their annual certification while they continued to represent themselves as current members. As discussed further below, the FTC also commits to addressing false claims of participation in the Privacy Shield Framework. This strategic enforcement activity will complement the Department of Commerce's increased actions to verify compliance with program requirements for certification and re-certification, its monitoring of

---

[11] *See In the Matter of Google, Inc.,* No. C-4336 (F.T.C. Oct. 13 2011) (decision and order), *available at* https://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz; *In the Matter of Facebook, Inc.*, No. C-4365 (F.T.C. July 27, 2012) (decision and order), *available at* https://www.ftc.gov/news-events/press-releases/2012/08/ftc-approves-final-settlement-facebook; *In the Matter of Myspace LLC*, No. C-4369 (F.T.C. Aug. 30, 2012) (decision and order), *available at* https://www.ftc.gov/news-events/press-releases/2012/09/ftc-finalizes-privacy-settlement-myspace.

[12] *See* Press Release, Fed. Trade Comm'n, Thirteen Companies Agree to Settle FTC Charges They Falsely Claimed to Comply with International Safe Harbor Framework (Aug. 17, 2015), *available at* https://www.ftc.gov/news-events/press-releases/2015/08/thirteen-companies-agree-settle-ftc-charges-they-falsely-claimed (Just Bagels Manufacturing, Inc.; Pinger, Inc.; NAICS Association, LLC; Golf Connect, LLC); Press Release, Fed. Trade Comm'n, FTC Settles with Two Companies Falsely Claiming to Comply with International Safe Harbor Framework (April 7, 2015), *available at* https://www.ftc.gov/news-events/press-releases/2015/04/ftc-settles-two-companies-falsely-claiming-comply-international (TES Franchising, LLC); Press Release, Fed. Trade Comm'n, FTC Approves Final Orders Settling Charges of U.S.-EU Safe Harbor Violations Against 14 Companies (June 25, 2014), *available at* https://www.ftc.gov/news-events/press-releases/2014/06/ftc-approves-final-orders-settling-charges-us-eu-safe-harbor (American Apparel, Inc.; Apperian, Inc.; Level 3 Communications, LLC; DataMotion, Inc.); *In the Matter of Myspace LLC*, No. C-4369 (F.T.C. Aug. 30, 2012) (decision and order), *available at* https://www.ftc.gov/news-events/press-releases/2012/09/ftc-finalizes-privacy-settlement-myspace.

effective compliance, including through the use of questionnaires to Framework participants, and its increased efforts to identify false Framework membership claims and misuse of any Framework certification mark.[13]

II. Referral Prioritization and Investigations

As we did under the Safe Harbor program, the FTC commits to give priority to Privacy Shield referrals from the Swiss Federal Data Protection and Information Commissioner ("Swiss DPA"). We will also prioritize referrals of non-compliance with self-regulatory guidelines relating to the Privacy Shield Framework from privacy self-regulatory organizations and other independent dispute resolution bodies.

To facilitate referrals under the Framework from Switzerland, the FTC is creating a standardized referral process and providing guidance to the Swiss DPA on the type of information that would best assist the FTC in its inquiry into a referral. As part of this effort, the FTC will designate an agency point of contact for Swiss DPA referrals. It is most useful when the referring authority has conducted a preliminary inquiry into the alleged violation and can cooperate with the FTC in an investigation.

Upon receipt of a referral from the Swiss DPA or a self-regulatory organization, the FTC can take a range of actions to address the issues raised. For example, we may review the company's privacy policies, obtain further information directly from the company 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 consumer and business education would be helpful, and, as appropriate, initiate an enforcement proceeding.

The FTC also commits to exchange information on referrals with the Swiss DPA, 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 Swiss DPA on the types of referrals received in order to increase the effectiveness of efforts to address unlawful conduct. If the Swiss DPA 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 Swiss DPA 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

[13] Letter from Ken Hyatt, Acting Under Secretary of Commerce for International Trade, International Trade Administration, to Federal Councillor Johann N. Schneider-Ammann, Head of the Department of Economic Affairs, Education and Research (Jan. 9, 2017).

similar to those prohibited by laws the FTC enforces.[14] As part of this assistance, the FTC can share information obtained in connection with an FTC investigation, issue compulsory process on behalf of the Swiss DPA conducting its own investigation, and seek oral testimony from witnesses or defendants in connection with the DPA'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.[15]

In addition to prioritizing Privacy Shield referrals from the Swiss DPA and privacy self-regulatory organizations,[16] the FTC commits to investigating possible Framework violations on its own initiative where appropriate using a range of tools.

For well over a decade, the FTC has maintained a robust program of investigating privacy and security issues involving commercial organizations. As part of these investigations, the FTC routinely examined whether the entity at issue was making Safe Harbor representations. If the entity was making such representations and the investigation revealed apparent violations of the Safe Harbor Privacy Principles, the FTC included allegations of Safe Harbor violations in its enforcement actions. We will continue this proactive approach under the new Framework. Importantly, the FTC conducts many more investigations than ultimately result in public enforcement actions. Many FTC investigations are closed because staff does not identify an apparent law violation. Because FTC investigations are non-public and confidential, the closing of an investigation is often not made public.

The nearly 40 enforcement actions initiated by the FTC involving the U.S.-EU and U.S.-Swiss Safe Harbor programs evidence the agency's commitment to proactive enforcement of cross-border privacy programs. The FTC will look for potential Framework violations as part of the privacy and security investigations we undertake on a regular basis.

---

[14] 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.

[15] In fiscal years 2012-2015, for example, the FTC used its U.S. SAFE WEB Act authority to share information in response to almost 60 requests from foreign agencies and it issued nearly 60 civil investigative demands (equivalent to administrative subpoenas) to aid 25 foreign investigations.

[16] Although the FTC does not resolve or mediate individual consumer complaints, the FTC affirms that it will prioritize Privacy Shield referrals from the Swiss DPA. 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. Swiss individuals can use the same complaint system available to U.S. consumers to submit a complaint to the FTC at www.ftc.gov/complaint. For individual Privacy Shield complaints, however, it may be most useful for Swiss individuals to submit complaints to the Swiss DPA or an alternative dispute resolution provider.

III. Addressing False or Deceptive Privacy Shield Membership Claims

As referenced above, the FTC will take action against entities that misrepresent their participation in the Framework. The FTC will give priority consideration to referrals from the Department of Commerce regarding organizations that it identifies as improperly holding themselves out to be current members of the Framework or using any Framework certification mark without authorization.

In addition, we note that if an organization's privacy policy promises that it complies with the Privacy Shield Principles, its failure to make or maintain a registration with the Department of Commerce likely will not, by itself, excuse the organization from FTC enforcement of those Framework commitments.

IV. Order Monitoring

The FTC also affirms its commitment to monitor enforcement orders to ensure compliance with the Privacy Shield Framework.

We will require compliance with the Framework through a variety of appropriate injunctive provisions in future FTC Framework orders. This includes prohibiting misrepresentations regarding the Framework and other privacy programs when these are the basis for the underlying FTC action.

The FTC's cases enforcing the original Safe Harbor program are instructive. In the 36 cases involving false or deceptive claims of Safe Harbor certification, each order prohibits the defendant from misrepresenting its participation in Safe Harbor or any other privacy or security program and requires the company to make compliance reports available to the FTC. In cases that involved violations of Safe Harbor Privacy Principles, companies have been required to implement comprehensive privacy programs and obtain independent third-party assessments of those programs every other year for twenty years, which they must provide to the FTC.

Violations of the FTC's administrative orders can lead to civil penalties of up to $40,000 per violation, or $40,000 per day for a continuing violation,[17] 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 Safe Harbor orders, as it does with all of its orders. The FTC takes enforcement of its privacy and data security orders seriously and brings actions to enforce them when necessary. For example, as noted above, Google paid a $22.5 million civil penalty to resolve allegations it had violated its FTC order. Importantly, FTC orders will continue to protect all consumers worldwide who interact with a business, not just those consumers who have lodged complaints.

[17] 15 U.S.C. § 45(m); 16 C.F.R. § 1.98.

Finally, the FTC will continue to maintain an online list of companies subject to orders obtained in connection with enforcement of both the Safe Harbor program and the new Privacy Shield Framework.[18] In addition, the Privacy Shield Principles now require companies subject to an FTC or court order based on non-compliance with the Principles to make public any relevant Framework-related sections of any compliance or assessment report submitted to the FTC, to the extent consistent with confidentiality laws and rules.

V. Engagement With the Swiss DPA and Enforcement Cooperation

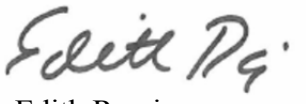
The FTC recognizes the important role that the Swiss DPA plays with respect to Framework compliance, and encourages increased consultation and enforcement cooperation. In addition to any consultation with the Swiss DPA on referral-specific matters, the FTC commits to participate in periodic meetings with the Swiss DPA to discuss in general terms how to improve enforcement cooperation with respect to the Framework. The FTC will also participate in the annual review of the Framework to discuss its implementation.

The FTC also encourages the development of tools that will enhance enforcement cooperation with the Swiss DPA, as well as other privacy enforcement authorities around the world. In particular, the FTC, along with enforcement partners in the European Union and around the globe, last year launched an alert system within the Global Privacy Enforcement Network ("GPEN") to share information about investigations and promote enforcement coordination. This GPEN Alert tool could be particularly useful in the context of the Privacy Shield Framework. The FTC and the Swiss DPA could use it to coordinate with respect to the Framework and other privacy investigations, including as a starting point for sharing information in order to deliver coordinated and more effective privacy protection for consumers. We look forward to continuing to work with participating authorities to deploy the GPEN Alert system more broadly and develop other tools to improve enforcement cooperation in privacy cases, including those involving the Framework.

***

The FTC is pleased to affirm its commitment to enforcing the new Privacy Shield Framework. We also look forward to continuing engagement with our Swiss colleagues as we work together to protect consumer privacy.

Sincerely,



Edith Ramirez
Chairwoman

[18] *See* FTC, Business Center, Legal Resources, https://www.ftc.gov/tips-advice/business-center/legal-resources?type=case&field_consumer_protection_topics_tid=251.