OFFICE OF CHAIRWOMAN
EDITH RAMIREZ

United States of America
FEDERAL TRADE COMMISSION
WASHINGTON, DC 20580

Commission in an effort to strengthen the privacy protections provided to EU citizens. The Privacy Shield Framework is a result of these ongoing consultations. As was the case with the Safe Harbor program, the FTC hereby commits to vigorous enforcement of the new Framework. This letter memorializes that commitment.

Notably, we affirm our 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 with EU DPAs. We provide below detailed information about each of these commitments and relevant background about the FTC's role in protecting consumer privacy and enforcing Safe

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

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.[6] 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.[7]

The FTC's settlement with TRUSTe is another example. It ensures that consumers, including those in the European Union, can rely on representations that a global self-regulatory organization makes about its review and certification of domestic and foreign online services.[8] Importantly, our action against TRUSTe also strengthens the privacy self-regulatory system more broadly by ensuring the accountability of entities that play an important role in self-regulatory schemes, including cross-border privacy frameworks.

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. In addition to the U.S. federal laws enforced by the FTC, certain other federal and state consumer protection and privacy laws may provide additional benefits to EU consumers.

C. Safe Harbor Enforcement

As part of its privacy and security enforcement program, the FTC has also sought to protect 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.[9] 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

[6] *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 fileb6305 -1.144 Tr65 -1.14rnap6d -35.305 -1.144 Td[b Tdp1(65 -11( )6(Cia)8.6c)]Tus c)]Tuariab T.2(2.3(

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 Privacy Shield Framework. The FTC can enforce these orders by seeking civil penalties. In f

To facilitate referrals under the Framework from EU Member States, the FTC is creating a standardized referral process and providing guidance to EU Member States 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

In addition to prioritizing Privacy Shield re

The FTC also encourages the development of tools that will enhance enforcement cooperation with EU DPAs, 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 EU DPAs 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 EU 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 EU colleagues as we work together to protect consumer privacy on both sides of the Atlantic.

Sincerely,

Edith Ramirez
Chairwoman