(As Prepared for Delivery)

Acting Chairman Maureen Ohlhausen
Transatlantic cooperation on personal privacy and data protection –
the EU/US Privacy Shield
FT Cyber Security Summit USA
National Press Club - 529 14th St NW - 13th Floor
Wednesday, March 15, 2017 at 11:20AM

Thank you for having me here today to discuss the status of our vital relationship with Europe and the work that we at the FTC are doing to preserve important data flows while protecting the privacy and data security of consumers on both sides of the Atlantic.

Last summer, U.S. and European Commission officials reached an agreement on the EU-U.S. Privacy Shield Framework. The Framework provides strong privacy protections for EU citizens and establishes an important mechanism for transatlantic data transfers. Since the launch of the system last August, over 1700 organizations have joined. Recently U.S. and Swiss officials have also finalized the Swiss-U.S. Privacy Shield, which aligns with the EU system.

When companies join Privacy Shield, they commit to follow the Privacy Shield principles. These include protections related to notice, choice, security, purpose limitation, and individual recourse. This new framework contains several improvements over the previous EU-U.S. data transfer framework, known as Safe Harbor. Privacy Shield has increased transparency: the Department of Commerce, which administers the program, developed a new website (privacyshield.gov) with sections aimed at US and European Businesses, EU individuals, and European Data Protection Authorities. Under Privacy Shield, there are more extensive verifications by Commerce of the self-certifications companies make when joining. There are more avenues for individual consumer redress, including free dispute resolution, complaint facilitation by Commerce and, when complaints remain unresolved, binding arbitration at the consumer's choice. There are also enhancements to the Principles, such as more explicit requirements for notice in privacy policies and additional requirements for third-party transfers.

The FTC plays a significant enforcement role in the framework, enforcing the promises that companies make when they join. The FTC is the chief privacy enforcer in the United States. We enforce a general law prohibiting unfair or deceptive practices across the commercial sector, as well as a wide range of sector-specific privacy and data security laws that protect health, financial, and children's information. We have brought over 500 cases protecting the privacy and security of consumer data.

Enforcing international privacy frameworks such as Privacy Shield is an integral part of our Data Security and Privacy program. We have used our authority to take action against nearly 40 companies for deceptively misrepresenting compliance with the predecessor Safe Harbor program, including Google and Facebook. We have also enforced against four companies that misrepresented their participation in the APEC Cross-border Privacy Rules System – a framework designed to facilitate data transfers in the Asia-Pacific region.

Based on this background, our deep history of privacy enforcement, and our commitment to interoperable international privacy frameworks, we will vigorously enforce the Privacy Shield Framework. We have committed to investigate Privacy Shield companies on our own initiative. We will prioritize referrals from European Data Protection authorities. And we will monitor our orders to ensure compliance with the Framework. When companies don't comply with orders, we will bring enforcement actions.

Let me expand a bit on how we are committed to cooperate on Privacy Shield enforcement. We're making the referral process clearer and easier: We created a standardized process and provided guidance to EU Member states on referrals. We also identified a designated agency point of contact for DPA referrals.

We're committing to using our authority, where appropriate, to share information and provide investigative assistance to DPAs. The U.S. SAFE WEB Act, which did not exist when Safe Harbor was set up in 2000, enhances our ability to cooperate on investigations with foreign agencies.

We're also committing to engage in ongoing discussions with the European institutions on the effectiveness of the Framework. We will participate in periodic meetings with designated representatives of the Article 29 Working Party to discuss how to improve enforcement cooperation under the Framework. We will also participate in the annual review of the Framework, along with the Department of Commerce and the European Commission.

Our transatlantic work is not limited to the Privacy Shield. The FTC has a strong history of cooperation on transatlantic privacy. We engage with our European counterparts both bilaterally and multilaterally.

We have Memoranda of Understanding with the UK, the Irish, and the Dutch privacy authorities. These Memoranda recognize that there are increasing cross-border data flows, and that effective privacy protection is promoted when privacy agencies engage in mutual assistance and information sharing. The MOUs facilitate exchanges on best practices, technological techniques, and staff expertise. One particular area we are excited to develop further is the possibility of staff exchanges with other privacy authorities. We recently had a technologist from the CNIL, the French DPA, on secondment with our technologists on cross-device tracking issues, and are looking for other such opportunities. These exchanges can help dispel common misunderstandings about U.S. privacy and data security framework by giving international counterparts hands-on experience with our vibrant enforcement and policy program.

We also participate in multinational fora like GPEN, the Global Privacy Enforcement Network. GPEN is working to develop deeper cooperation among privacy enforcement authorities. With over 60 participating agencies from over 45 countries, GPEN has conducted several global privacy sweeps, including last year's on the Internet of Things. GPEN organizes teleconferences and other events for the exchange of know-how among enforcement authorities. Several European authorities are GPEN participants. The UK's ICO is a particularly committed member: they join the FTC, Canada, Israel and Hong Kong in the GPEN Committee, which does much of the work of organizing the network. Significantly, the UK is organizing this year's GPEN sweep.

GPEN has also developed a powerful coordination tool for investigations. At the 2015 International Conference of Data Protection and Privacy Commissioners, the FTC and seven other privacy agencies from North America, Europe, and Asia-Pacific launched GPEN Alert, a secure information-sharing system for coordinating privacy investigations. A total of 10 agencies now participate. The UK ICO is one of the founding participants in GPEN Alert, and also donated funds for the development of the system. The system can be used for Privacy Shield investigations as well as for other secure exchanges.

The FTC is committed to our transatlantic relationships, in Privacy Shield and beyond. We all benefit from cross border data flows and the new and innovative services it enables. With these increasing data flows comes a greater need for cooperation among authorities to provide the effective privacy protections for our citizens on both sides of the Atlantic.

With that, thank you again for having me, and I'd be happy to take any questions at this time.