ATTACHMENT A

The EU-U.S. Privacy Shield Framework in Context:
An Overview of the U.S. Privacy and Security Landscape

The protections provided by the EU-U.S. Privacy Shield Framework (the "Framework") exist in the context of the broader privacy protections afforded under the U.S. legal system as a whole. First, the U.S. Federal Trade Commission ("FTC") has a robust privacy and data security program for U.S. commercial practices that protects consumers worldwide. Second, the landscape of consumer privacy and security protection in the United States has evolved substantially since 2000 when the original U.S.-EU Safe Harbor program was adopted. Since that time, many federal and state privacy and security laws have been enacted, and public and private litigation to enforce privacy rights has increased significantly. The broad scope of U.S. legal protections for consumer privacy and security applicable to commercial data practices complements the protections provided to EU individuals by the new Framework.

I. The FTC's General Privacy and Security Enforcement Program

The FTC is the leading U.S. consumer protection agency focused on commercial sector privacy. The FTC has authority to prosecute unfair and deceptive acts or practices that violate consumer privacy, as well as to enforce more targeted privacy laws that protect certain financial and health information, information about children, and information used to make certain eligibility decisions about consumers.

The FTC has unparalleled experience in consumer privacy enforcement. The FTC's enforcement actions have addressed unlawful practices in offline and online environments. For example, the FTC has brought enforcement actions against well-known companies, such as Google, Facebook, Twitter, Microsoft, Wyndham, Oracle, HTC, and Snapchat, as well as lesser-known companies. The FTC has sued businesses that allegedly spammed consumers, installed spyware on computers, failed to secure consumers' personal information, deceptively tracked consumers online, violated children's privacy, unlawfully collected information on consumers' mobile devices, and failed to secure Internet-connected devices used to store personal information. The resulting orders have typically provided for ongoing monitoring by the FTC for a period of twenty years, prohibited further law violations, and subjected the businesses to substantial financial penalties for order violations.[1] Importantly, FTC orders do not just protect the individuals who may have complained about a problem; rather, they protect all consumers dealing with the business going forward. In the cross-border context, the FTC has jurisdiction to protect consumers worldwide from practices taking place in the United States.[2]

To date, the FTC has brought over 130 spam and spyware cases, over 120 "Do Not Call" telemarketing cases, over 100 Fair Credit Reporting Act actions, almost 60 data security cases, more than 50 general privacy actions, almost 30 cases for violations of the Gramm-Leach-Bliley

[1] Any entity that fails to comply with an FTC order is subject to a civil penalty of up to $16,000 per violation, or $16,000 per day for a continuing violation. *See* 15 U.S.C. § 45(l); 16 C.F.R. § 1.98(c).

[2] Congress has expressly affirmed the FTC's authority to seek legal remedies, including restitution, for any acts or practices involving foreign commerce that (1) cause or are likely to cause reasonably foreseeable injury in the United States, or (2) involve material conduct occurring within the United States. *See* 15 U.S.C. § 45(a)(4).

Act, and over 20 actions enforcing the Children's Online Privacy Protection Act ("COPPA").[3] In addition to these cases, the FTC has also issued and publicized warning letters.[4]

As part of its history of strong privacy enforcement, the FTC has also regularly looked for potential violations of the Safe Harbor program. Since the Safe Harbor program was adopted, the FTC has undertaken numerous investigations into Safe Harbor compliance on its own initiative and has brought 39 cases against U.S. companies for Safe Harbor violations. The FTC will continue this proactive approach by making enforcement of the new Framework a priority.

II. Federal and State Protections for Consumer Privacy

The Safe Harbor Enforcement Overview, which appears as an annex to the European Commission's Safe Harbor adequacy decision, provides a summary of many of the federal and state privacy laws in place at the time the Safe Harbor program was adopted in 2000.[5] At that time, many federal statutes regulated the commercial collection and use of personal information, beyond Section 5 of the FTC Act, including: the Cable Communications Policy Act, the Driver's Privacy Protection Act, the Electronic Communications Privacy Act, the Electronic Funds Transfer Act, the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act, the Right to Financial Privacy Act, the Telephone Consumer Protection Act, and the Video Privacy Protection Act. Many states had analogous laws in these areas as well.

Since 2000, there have been numerous developments at both the federal and state level that provide additional consumer privacy protections.[6] At the federal level, for example, the FTC amended the COPPA Rule in 2013 to provide a number of additional protections for children's personal information. The FTC also issued two rules implementing the Gramm-Leach-Bliley Act – the Privacy Rule and the Safeguards Rule – which require financial

---

[3] In some instances, the Commission's privacy and data security cases allege that a company engaged in both deceptive and unfair practices; these cases also sometimes involve alleged violations of multiple statutes, such as the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act, and COPPA.

[4] *See, e.g.*, Press Release, Fed. Trade Comm'n, FTC Warns Children's App Maker BabyBus About Potential COPPA Violations (Dec. 22, 2014), https://www.ftc.gov/news-events/press-releases/2014/12/ftc-warns-childrens-app-maker-babybus-about-potential-coppa; Press Release, Fed. Trade Comm'n, FTC Warns Data Broker Operations of Possible Privacy Violations (May 7, 2013), https://www.ftc.gov/news-events/press-releases/2013/05/ftc-warns-data-broker-operations-possible-privacy-violations; Press Release, Fed. Trade Comm'n, FTC Warns Data Brokers That Provide Tenant Rental Histories They May Be Subject to Fair Credit Reporting Act (Apr. 3, 2013), https://www.ftc.gov/news-events/press-releases/2013/04/ftc-warns-data-brokers-provide-tenant-rental-histories-they-may.

[5] *See* U.S. Dep't of Commerce, Safe Harbor Enforcement Overview, https://build.export.gov/main/safeharbor/eu/eg_main_018481.

[6] For a more comprehensive summary of the legal protections in the United States, see Daniel J. Solove & Paul Schwartz, *Information Privacy Law* (5th ed. 2015).

institutions[7] to make disclosures about their information sharing practices and to implement a comprehensive information security program to protect consumer information.[8] Similarly, the Fair and Accurate Credit Transactions Act ("FACTA"), enacted in 2003, supplements longstanding U.S. credit laws to establish requirements for the masking, sharing, and disposal of certain sensitive financial data. The FTC promulgated a number of rules under FACTA regarding, among other things, consumers' right to a free annual credit report; secure disposal requirements for consumer report information; consumers' right to opt out of receiving certain offers of credit and insurance; consumers' right to opt out of the use of information provided by an affiliated company to market its products and services; and requirements for financial institutions and creditors to implement identity theft detection and prevention programs.[9] In addition, rules promulgated under the Health Insurance Portability and Accountability Act were revised in 2013, adding additional safeguards to protect the privacy and security of personal health information.[10] Rules protecting consumers from unwanted telemarketing calls, robocalls, and spam have also gone into effect. Congress has also enacted laws requiring certain companies that collect health information to provide consumers with notification in the event of a breach.[11]

States have also been very active in passing laws related to privacy and security. Since 2000, forty-seven states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted laws requiring businesses to notify individuals of security breaches of personal information.[12] At least thirty-two states and Puerto Rico have data disposal laws, establishing requirements for the destruction or disposal of personal information.[13] A number of states also have enacted general data security laws. In addition, California has enacted various privacy laws, including a law requiring companies to have privacy policies and disclose their Do Not

---

[7] Financial institutions are defined very broadly under the Gramm-Leach-Bliley Act to include all businesses that are "significantly engaged" in providing financial products or services. This includes, for example, check-cashing businesses, payday lenders, mortgage brokers, nonbank lenders, personal property or real estate appraisers, and professional tax preparers.

[8] Under the Consumer Financial Protection Act of 2010 ("CFPA"), Title X of Pub. L. 111-203, 124 Stat. 1955 (July 21, 2010) (also known as the "Dodd-Frank Wall Street Reform and Consumer Protection Act"), most of the FTC's Gramm-Leach-Bliley Act rulemaking authority was transferred to the Consumer Financial Protection Bureau ("CFPB"). The FTC retains enforcement authority under the Gramm-Leach-Bliley Act as well as rulemaking authority for the Safeguards Rule and limited rulemaking authority under the Privacy Rule with respect to auto dealers.

[9] Under the CFPA, the Commission shares its FCRA enforcement role with the CFPB, but rulemaking authority transferred in large part to the CFPB (with the exception of the Red Flags and Disposal Rules).

[10] *See* 45 C.F.R. pts. 160, 162, 164.

[11] *See, e.g.*, American Recovery & Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (2009) and relevant regulations, 45 C.F.R. §§ 164.404-164.414; 16 C.F.R. pt. 318.

[12] *See, e.g.*, National Conference of State Legislatures ("NCSL"), *State Security Breach Notification Laws* (Jan. 4, 2016), *available at* http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx .

[13] NCSL, *Data Disposal Laws* (Jan. 12, 2016), *available at* http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx.

Track practices,[14] a "Shine the Light" law requiring greater transparency for data brokers,[15] and a law that mandates an "eraser button" allowing minors to request the deletion of certain social media information.[16] Using these laws and other authorities, federal and state governments have levied significant fines against companies that have failed to protect the privacy and security of consumers' personal information.[17]

Private lawsuits have also led to successful judgments and settlements that provide additional privacy and data security protection for consumers. For example, in 2015, Target agreed to pay $10 million as part of a settlement with customers who claimed their personal financial information was compromised by a widespread data breach. In 2013, AOL agreed to pay a $5 million settlement to resolve a class action involving alleged inadequate de-identification related to the release of search queries of hundreds of thousands of AOL members. Additionally, a federal court approved a $9 million payment by Netflix for allegedly keeping rental history records in violation of the Video Privacy Protection Act of 1988. Federal courts in California approved two separate settlements with Facebook, one for $20 million and another for $9.5 million, involving the company's collection, use, and sharing of its users' personal information. And, in 2008, a California state court approved a $20 million settlement with LensCrafters for unlawful disclosure of consumers' medical information.

In sum, as this summary illustrates, the United States provides significant legal protection for consumer privacy and security. The new Privacy Shield Framework, which ensures meaningful safeguards for EU individuals, will operate against this larger backdrop in which the protection of consumers' privacy and security continues to be an important priority.

---

[14] Cal. Bus. & Professional Code §§ 22575-22579.

[15] Cal. Civ. Code §§ 1798.80-1798.84.

[16] Cal. Bus. & Professional Code § 22580-22582.

[17] *See* Jay Cline, *U.S. Takes the Gold in Doling Out Privacy Fines*, Computerworld (Feb. 17, 2014), *available at* http://www.computerworld.com/s/article/9246393/Jay_Cline_U.S._takes_the_gold_in_doling_out_privacy_fines?taxonomyId=17&pageNumber=1.