U.S. Privacy Law: Hiding in Plain Sight
U.S. Federal Trade Commissioner Julie Brill
Second German-American Data Protection Day
Munich, Germany
April 30, 2015

Thank you, Dr. Ehmann, for your kind introduction. I am pleased to be part of today's celebration of the second German-American Data Protection Day, and I am delighted to discuss the U.S.-EU Safe Harbor and transatlantic data transfers.

As eager as I am to get to the important topic of data flows between the United States, Germany, and the rest of the European Union, I would like to lay a foundation for that conversation. In particular, I would like to provide you with an overview of the strong privacy laws in the United States and the efforts of my agency, the U.S. Federal Trade Commission (FTC), to enforce those laws.

The FTC is the leading consumer protection agency in the United States. We are primarily a law enforcement agency, and we are independent of the Administration. All five Commissioners are appointed by the President, and confirmed by the Senate for a set term – usually seven years. We are bipartisan – no more than three Commissioners can be from the same political party. We have over 1,000 attorneys, economists, technologists and support staff engaged in our law enforcement and policy development efforts. We focus on a broad swath of the economy, and bring enforcement actions involving anticompetitive mergers and acquisitions and other anticompetitive practices, as well as cases involving advertising substantiation, telemarketing fraud, payment systems – including new mobile payment systems, and other practices that cause consumers financial harm.[1]

Despite that very broad mandate, privacy and data security are among our highest priorities. Since the late 1990s, the FTC has brought more than 40 privacy-related enforcement actions and approximately 55 data security enforcement actions under the general consumer protection authority granted by Section 5 of the FTC Act.[2] The FTC has taken action against some of the biggest Internet companies in the world including, Google, Facebook, Twitter, and Snapchat. We have also brought cases against companies that are not household names but violated the law by deceptively tracking consumers online, putting spyware on their computers, or violating consumers' privacy in other ways.

In addition, the FTC has brought 26 actions against companies specifically for violating the U.S.-EU Safe Harbor agreement.[3] Our actions against Google and Facebook also included

[1] *See generally* FTC, 2014 Annual Highlights: Stats & Data, *available at* https://www.ftc.gov/annual-highlights-2014/stats-data-2014 (last visited Apr. 29, 2015).

[2] *See* FTC, Privacy & Security Update (2014), *available at* http://www.ftc.gov/reports/privacy-data-security-update-2014 ["2014 Privacy & Security Update"].

[3] True Ultimate Standards Everywhere (TRUSTe), No. C-4512 (F.T.C. Mar. 12, 2015), ¶¶ 11-16 (complaint), *available at* https://www.ftc.gov/system/files/documents/cases/150318trust-ecmpt.pdf. UTrue Ultimate Standards Everywhere (TRUSTe), No. C-4512 (F.T.C. Mar. 12, 2015), ¶¶ 11-16 (complaint), *available at* https://www.ftc.gov/system/files/documents/cases/150318trust-ecmpt.pdf; FTC, Press Release, FTC Approves Final

allegations that those companies violated their Safe Harbor commitments. FTC enforcement helps protect the privacy of millions of EU citizens as a result. The FTC Act, and in particular Section 5 of the Act, is the law that stands behind these Safe Harbor actions, so understanding how Section 5 enforcement works is essential to the discussion we're having today.

But first it is important to note that privacy protections in the United States do not begin and end with this one law. Section 5 is only one strand of the strong fabric of U.S. privacy law. At the federal level, the U.S. has enacted privacy protections that apply to specific activities or economic sectors, such as healthcare,[4] banking,[5] credit reporting,[6] and communications.[7] Other federal laws protect children's privacy[8] and students' privacy.[9] In addition, individual states are active privacy regulators. Last year, approximately 60 new privacy laws were passed at the state level in the U.S. State privacy laws range from limiting employers' ability to view their employees' social network accounts[10] and prohibiting employers and insurers from using information about certain medical conditions,[11] to requiring companies to notify consumers when they suffer a security breach involving personal information.[12]

Compared to the specificity of these other U.S. privacy laws, as well as the European Data Privacy Directive, Section 5 looks a little unusual. Section 5 does not mention the words "privacy" or "personal data". Instead, Section 5 outlaws "unfair or deceptive acts or practices."[13] When Congress added these provisions to the FTC Act in 1938, it understood that harmful deception, fraud and unfair treatment can change quickly, as technology and business practices evolve. To ensure that the FTC could keep up with these changes, Congress gave the FTC broad, flexible authority to remedy harms to consumers in the market place.

Order in TRUSTe Case (Mar. 18, 2015), available at https://www.ftc.gov/news-events/press-releases/2015/03/ftc-approves-final-order-truste-privacy-case.

[4] Health Insurance Portability and Accountability Act, Pub. L. No.104-191, 110 Stat. 1936 (1996) (codified in scattered sections of 18, 26, 29, and 42 U.S.C.).

[5] 15 U.S.C. §§ 6801-09.

[6] 15 U.S.C. § 1681 *et seq.*

[7] 47 U.S.C. §§ 222, 338, and 631.

[8] *See* Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-06.

[9] Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g.

[10] *See* Nat'l Conf. of State Legislatures, Employer Access to Social Media Usernames and Passwords, available at http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013.aspx (last updated Nov. 18, 2014) (noting that in 2014, at least 28 states had introduced social media and employment legislation or had such legislation pending).

[11] *See, e.g.*, Privacy Rights Clearinghouse, *California Medical Privacy Fact Sheet C5: Employment and Your Medical Privacy*, *available at* https://www.privacyrights.org/content/employment-and-your-medical-privacy (last updated July 2012).

[12] *See* Nat'l Conf. of State Legislatures, Security Breach Notification Laws (Jan. 12, 2015), *available at* http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (collecting references to more than 45 state laws).

[13] 15 U.S.C. § 45(a), *available at* https://www.law.cornell.edu/uscode/text/15/45. .

The FTC first began to apply Section 5 to companies' privacy and data security practices two decades ago, it was clear that the personal data flowing as part of electronic commerce could be used to cause financial harm to consumers. But it was also clear – even back then – that personal data practices could cause a much broader array of harms.[14] Today, as more and more information about our online and offline activities, health, finances, friends, and families is readily available, Section 5's prohibition against unfair or deceptive practices remains a durable source of protection against inappropriate data collection, use, and disclosure.

Let me first discuss how we use our authority over deceptive practices to protect consumers' privacy. When a company tells consumers what personal data it collects, how it uses this data, and to whom it is disclosed, those representations must be truthful. When a company says one thing in its privacy policy but does something else, that's a straightforward case of deception. For example, if a company says it does not disclose personal data to third parties but in fact it does, then the company may be inviting a law enforcement action from the FTC.[15]

There is another side to our authority to police deceptive practices. What a company *does not* tell consumers may be just as important as what it states expressly. In other words, omissions can also be deceptive. In one recent case, for example, the FTC charged that the producer of a mobile app that turns the phone's camera flash bulb into a flashlight inappropriately neglected to tell consumers that the app collected precise location information, persistent identifiers, and other personal and sensitive information that consumers would not expect to flow from a flashlight app.[16] In another deceptive omission case, we charged that an online ad network deceived consumers when it offered an opt-out but failed to state that the opt-out lasted for only 10 days.[17]

Some critics of U.S. privacy law argue that it is fundamentally a system in which companies volunteer to be subject to legal enforcement, and if a company doesn't make any promises about its activity, it will not be subject to any kind of privacy regulation. This view is mistaken, for a few reasons. First, this view ignores the important sector-specific laws governing data of heightened sensitivity, such as medical, financial and credit reporting information, and information about children and students.[18] Second, the FTC's unfairness authority provides a separate basis for privacy enforcement under the broad and remedial FTC Act. An unfair practice is one that causes substantial injury to consumers, is not reasonably avoidable, and does

---

[14] *See, e.g.*, FTC, Press Release, Eli Lilly Settles FTC Charges Concerning Security Breach (Jan. 18, 2002), *available at* https://www.ftc.gov/news-events/press-releases/2002/01/eli-lilly-settles-ftc-charges-concerning-security-breach.

[15] *See, e.g.*, Facebook, Inc., No. C-4365 (F.T.C. July 27, 2012) ¶¶ 34-42 (complaint), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookcmpt.pdf (alleging that Facebook "provided advertisers with information about its users" in violation of representations to the contrary) ["Facebook Complaint"].

[16] *See* Goldenshores Techs., LLC, C-4466 (F.T.C. Mar. 31, 2014) ¶¶ 11-12 (complaint), *available at* https://www.ftc.gov/system/files/documents/cases/140409goldenshorescmpt.pdf.

[17] *See* Chitika, Inc., No. C-4323 (F.T.C. June 7, 2011) ¶¶ 9-13 (complaint), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2011/06/110617chitikacmpt.pdf.

[18] *See supra* notes 4-9 and accompanying text.

not have offsetting benefits. We use unfairness in cases that meet this standard, even if a company has said nothing about the practice at issue. The FTC has used its unfairness authority to take action against companies that materially changed how they use personal data they have already collected without getting consumers' permission, as in our case against Facebook.[19] We have also used our unfairness authority against companies that we believed failed to provide reasonable data security,[20] or set default permissions on apps that were so permissive and difficult to undo that consumers unwittingly ended up sharing files on their smartphones.[21]

As I mentioned earlier, Section 5 also provides the authority for the FTC to enforce the promises that companies make when they join the Safe Harbor program. Companies that want to be in Safe Harbor must certify and publicly declare that they follow the seven Safe Harbor privacy principles in their own data practices. The FTC has settled 26 actions against companies that we believed either falsely stated that they were in Safe Harbor but actually were not, or claimed to meet Safe Harbor's substantive requirements but did not.[22] In addition, the FTC brought an action against TRUSTe, which maintains a Safe Harbor certification program, over its alleged misrepresentations about the extent to which it conducted annual recertifications for Safe Harbor and other privacy programs.[23] By holding companies to their Safe Harbor commitments, and taking action against other key participants in the Safe Harbor program, the FTC has improved privacy protections for EU citizens.

Whether an FTC enforcement action involves unfairness or deception – or both – it is serious business. Our privacy and data security cases generally end with legally binding orders that require companies to fix the problems that underlie our complaints and avoid future missteps in their data practices. In some instances, our orders require companies to set up and maintain comprehensive privacy or security programs. Orders typically last for 20 years, and companies face fines if they violate them. Indeed, we brought such an action against Google, which paid a $22.5 million penalty to settle our allegation that it violated a prior – arising from its rollout of the Buzz social network – by misrepresenting to users of Apple's web browser that Google would not place tracking cookies or serve targeted ads to those users.[24]

---

[19] *See, e.g.*, Facebook Complaint, *supra* note 15, at ¶ 29.

[20] See, e.g., *See* GMR Transcription Servs., No. C-4482 (F.T.C. Aug.14, 2014) (consent order), *available at* https://www.ftc.gov/system/files/documents/cases/140821gmrdo.pdf.

[21] FTC v. Frostwire LLC, Case No. 1:11-cv-23463 (S.D. Fla., Oct. 7, 2011) ¶¶ 25-31, 41-43 (complaint), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111011frostwirecmpt.pdf.

[22] *See* 2014 Privacy & Security Update, *supra* note 2 (noting that "[s]ince 2009 the FTC has used Section 5 to bring 24 Safe Harbor cases").

[23] True Ultimate Standards Everywhere (TRUSTe), No. C-4512 (F.T.C. Mar. 12, 2015), ¶¶ 11-16 (complaint), *available at* https://www.ftc.gov/system/files/documents/cases/150318trust-ecmpt.pdf. Under the FTC's order, TRUSTe is prohibited from making such representations and is subject to civil penalties if it fails to abide by these terms. *See* TRUSTe, No. 4512 (F.T.C. Mar. 12, 2015) (consent order), *available at* https://www.ftc.gov/system/files/documents/cases/150318trust-edo.pdf.

[24] *See* FTC, Press Release, Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser (Aug. 9, 2012), *available at* https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented.

Finally, the FTC's privacy and data security work goes beyond law enforcement. We constantly examine changes in technology and business practices that affect consumers – both positively and negatively. As big data and data-driven decision-making have become more sophisticated and relevant to consumers, the FTC has led several efforts to promote public discussion and debate about these issues. We have held public workshops on methods for scoring consumers, maintaining the privacy and security of health information generated by consumers, and how big data can be a tool for inclusion and a tool for discrimination. In addition, in the last year, the FTC has issued two landmark reports on aspects of the data-driven economy. In May 2014, we published an in-depth study of the data broker industry, which includes detailed recommendations to Congress and to industry on how to make this industry more transparent and accountable.[25] And in January, we published a report on the Internet of Things, which draws attention to the fundamental importance of data security and providing appropriate safeguards for sensitive information as everyday objects, from cars to refrigerators, become connected to the Internet.[26]

Now that I have laid out the basics of U.S. privacy law and FTC enforcement, including Safe Harbor enforcement, I look forward to the discussion with all of you. Thank you.

[25] FTC, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY (2014), *available at* http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

[26] *See generally* FTC, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD 19-22 (2015) (staff report), *available at* http://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf (discussing views of workshop participants).