

UNITED STATES OF AMERICA  
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: Edith Ramirez, Chairwoman  
Julie Brill  
Maureen K. Ohlhausen  
Joshua D. Wright



\_\_\_\_\_ ) DOCKET NO. 9357  
In the Matter of )  
 )  
LabMD, Inc., ) PUBLIC  
a corporation. )  
\_\_\_\_\_ )

**RESPONDENT'S MOTION TO DISQUALIFY COMMISSIONER BRILL  
FROM THIS ADMINISTRATIVE PROCEEDING**

Pursuant to Commission Rule 4.17, 16 C.F.R. § 4.17, Respondent LabMD, Inc. (LabMD) respectfully moves for the disqualification of Commissioner Julie Brill from this matter because her public statements show she has prejudged the facts of LabMD's case.

In a September 17, 2013, keynote address to Forum Europe in Brussels, Belgium, Commissioner Brill said FTC has "brought myriad cases against companies that are not household names, but whose practices crossed the line." She called out LabMD by name as the leading example of companies FTC challenged for "fail[ing] to properly secure consumer information." Forum Europe Fourth Annual EU Data Protection and Privacy Conference, Commissioner Julie Brill's Keynote Address, at 3 & n.15 (Sept. 17, 2013) (citing *In the Matter of LabMD*, FTC File No. 102 3099 (Aug. 28, 2013) (administrative complaint) (Ex. A).

On October 29, 2013, Commissioner Brill used even more damning language, stating: "We ... have brought myriad cases against companies ... *whose practices [have] violated the law.* We've sued companies that ... failed to secure consumers' personal information." Commissioner Julie Brill's Opening Panel Remarks, European Institute, "Data Protection,

Privacy and Security: Re-Establishing Trust Between Europe and the United States,” at 3 & n.15 (Oct. 29, 2013) (emphasis added) (Ex. B). Commissioner Brill then, once again for emphasis, cited LabMD as the leading and only culprit. *Id.* (citing *In the Matter of LabMD*, FTC File No. 102 3099 (Aug. 28, 2013) (administrative complaint)).

*With the exception of the LabMD matter*, each Commission matter that Commissioner Brill cited as examples of Section 5 violations in the foregoing speeches is a final decision of some kind:<sup>1</sup> “decision and order”; “consent decree and order”; “stipulated final order”; “agreement containing consent order”; “stipulated final order”; an Article III court’s order. *See* Ex. A at 3-4 & nn. 11-23; Ex. B. at 3 nn. 9-19. *In the Matter of LabMD*, FTC File No. 102 3099 (Aug. 28, 2013), is a pending case before the Commission (including Commissioner Brill); LabMD has denied violating Section 5 and has exercised its right to a hearing before an ALJ; the ALJ has not made any factual findings as to LabMD’s Section 5 liability; and LabMD has filed a Motion to Dismiss with Prejudice that is currently pending before the Commission (which Commissioner Brill, along with the other Commissioners, will rule on absent disqualification).

The test for disqualification is whether “a disinterested observer may conclude that [the agency] has in some measure adjudged the facts as well as the law of a particular case in advance of hearing it.”<sup>2</sup> *Cinderella Career & Finishing Schools, Inc. v. FTC*, 425 F.2d 583, 591 (D.C. Cir. 1970); *see also Nuclear Info. & Res. Serv. v. NRC*, 509 F.3d 562, 571 (D.C. Cir. 2007) (agency official should be disqualified when the “disinterested observer” standard has been met under *Cinderella*, i.e., the official “has in some measure adjudged the facts as well as the law of a

---

<sup>1</sup> Undersigned counsel learned of Commissioner Brill’s statements on Sunday, December 15, 2013.

<sup>2</sup> “[O]ur system of law has always endeavored to prevent even the probability of unfairness.” *In re Murchison*, 349 U.S. 133, 136-37 (1955). “[T]he Due Process Clause has been implemented by objective standards that do not require proof of actual bias.” *Caperton v. A. T. Massey Coal Co.*, 556 U.S. 868, 883-84 (2009).

particular case in advance of hearing it”); *Metropolitan Council of NAACP Branches v. FCC*, 46 F.3d 1154, 1164-65 (D.C. Cir. 1995) (citing *Cinderella* as the standard). Here, that test has been more than met. Commissioner Brill has told the world that LabMD failed to secure consumer information and violated the law. Both of these conclusions, however, should properly follow an evidentiary hearing, not precede it.<sup>3</sup> No neutral judge with any regard for the due process-requirement of avoiding the appearance of bias and prejudgment would ever say such things about a pending case.<sup>4</sup>

*Cinderella* therefore controls and mandates Commissioner Brill’s disqualification. There, as here, a FTC commissioner made statements suggesting he had prejudged a pending case. *See Cinderella*, 425 F.2d at 589-91. In *Cinderella*, the respondent’s business “operate[d] and grant[ed] franchises for the operation of schools offering various courses in modeling, fashion merchandising, charm, and self-improvement.” *FTC v. Cinderella Career & Finishing*

<sup>3</sup> Cf. Michael D. Pepson & John N. Sharifi, *Lego v. Twombly: The Improbable Relationship Between An Obscure Supreme Court Decision and Wrongful Convictions*, 47 AM. CRIM. L. REV. 1185, 1231-35 (2010) (arguing that institutional bias against defendants leads to erroneous factfinding and, in turn, wrongful convictions); Michael D. Pepson, Comment, *Therapeutic Jurisprudence in Philosophical Perspective*, 2 J. OF LAW, PHIL. & CULTURE 239, 260-64 (2008) (noting that the Supreme Court has said that due process requires a hearing that is more than a sham or a pretense).

<sup>4</sup> Commissioner Brill’s conclusory statements that LabMD has, *in fact*, violated Section 5 are markedly different from a factual press release stating that the Commission has issued a complaint after finding “*reason to believe*” that a Section 5 violation *may* have occurred. Commissioner Brill said these things about a *hotly contested high-profile case pending before her* without using words like “allegedly” and without mentioning that she was responsible for not only ruling on LabMD’s dispositive motions in the first instance but also deciding the matter *after* a full-blown administrative adjudication. “It is fundamental that both unfairness and the appearance of unfairness should be avoided. Wherever there may be reasonable suspicion of unfairness, it is best to disqualify.” *Am. Cyanamid Co. v. FTC*, 363 F.2d 757, 767 (6th Cir. 1966). *See generally Marshall v. Jerrico, Inc.*, 446 U.S. 238, 242 (1980) (The Due Process Clause’s “neutrality requirement[, *inter alia*,] preserves both the appearance and reality of fairness, generating the feeling, so important to a popular government, that justice has been done, by ensuring that no person will be deprived of his interests in the absence of a proceeding in which he may present his case with assurance that the arbiter is not predisposed to find against him.” (citation omitted)).

*Schools, Inc.*, 404 F.2d 1308, 1309 (D.C. Cir. 1968). FTC Chairman Dixon discussed the respondent's business model and allegedly unfair or deceptive practices in a thinly-veiled speech to a trade association and said:

What kind of vigor can a reputable newspaper exhibit? ... What standards are maintained on advertising acceptance? What would be the attitude toward accepting good money for advertising by a merchant who conducts a "going out of business" sale every five months? *What about carrying ads that offer college educations in five weeks, fortunes by raising mushrooms in the basement, getting rid of pimples with a magic lotion, or becoming an airline's hostess by attending a charm school?* Or, to raise the target a bit, how many newspapers would hesitate to accept an ad promising an unqualified guarantee for a product when the guarantee is subject to many limitations? .... *Granted that newspapers are not in the advertising policing business, their advertising managers are savvy enough to smell deception when the odor is strong enough.*

*Cinderella*, 425 F.2d at 589-90 (emphasis in original).

The *Cinderella* court disqualified Dixon for this, saying:

It requires no superior olfactory powers to recognize that the danger of unfairness through prejudgment is not diminished by a cloak of self-righteousness. We have no concern for or interest in the public statements of government officers, but we are charged with the responsibility of making certain that the image of the administrative process is not transformed from a Rubens to a Modigliani.

[T]here is in fact and law authority in the Commission, acting in the public interest, to alert the public to suspected violations of the law by factual press releases whenever the Commission shall have reason to believe that a respondent is engaged in activities made unlawful by the Act. *This does not give individual Commissioners license to prejudge cases or to make speeches which give the appearance that the case has been prejudged.* Conduct such as this may have the effect of entrenching a Commissioner in a position which he has publicly stated, making it difficult, if not impossible, for him to reach a different conclusion in the event he deems it necessary to do so after consideration of the record. There is a marked difference between the issuance of a press release which states that the Commission has filed a complaint because it has "reason to believe" that there have been violations, and statements by a Commissioner after an appeal has been filed *which give the appearance that he has already prejudged the case and that the ultimate determination of the merits will move in predestined grooves.* While these two situations—Commission press releases and a Commissioner's pre-decision public statements—are similar in appearance, they are obviously of a different order of merit.

*Id.* at 590 (emphasis added).

Commissioner Brill's statements are even more explicit and egregious than Dixon's. Commissioner Brill effectively stated that, in her view, LabMD's data-security practices, as a factual matter, violate Section 5. The above-cited statements were made shortly after Commissioner Brill voted to issue a Complaint against LabMD, and subsequent to LabMD's Answer denying any violation of Section 5. Commissioner Brill has thereby disposed of the fiction of FTC fairness and left no doubt about her position as to LabMD's eventual fate regardless of the outcome of its evidentiary hearing. Even before her statements, the evidence of futility was there for anyone who cared to peek inside FTC's procedural curtain and see. But Commissioner Brill has torn down this curtain and left FTC bare.

To begin with, FTC's administrative process appears to be rigged against respondents. The empirical data is that for nearly the past twenty years, in 100% of the cases where the ALJ ruled for FTC, the Commission affirmed, but in 100% of the cases where the ALJ ruled for respondent, the Commission reversed. In other words, FTC never loses.<sup>5</sup>

According to Commissioner Wright, the reason that the FTC's enforcement of Section 5 is fundamentally unfair arises from a combination of FTC's administrative process advantages and the vague nature of Section 5 authority. This toxic mixture gives FTC great power because, as Commissioner Wright recently told Congress, "firms typically prefer to settle Section 5 claims rather than go through the lengthy and costly administrative litigation in which they are both shooting at a moving target and may have the chips stacked against them." Preliminary Transcript, "The FTC at 100: Where Do We Go From Here?," House of Representatives,

---

<sup>5</sup> Wright, "Recalibrating Section 5: A Response to the CPI Symposium," CPI ANTITRUST CHRONICLE, 4 (Nov. 2013), available at <https://www.competitionpolicyinternational.com/> (accessed Dec. 15, 2013).

Subcommittee on Commerce, Manufacturing, and Trade, Committee on Energy and Commerce,  
at 34 (Dec. 3, 2013), available at  
[http://democrats.energycommerce.house.gov/sites/default/files/documents/Preliminary-  
Transcript-CMT-FTC-at-100-2013-12-3.pdf](http://democrats.energycommerce.house.gov/sites/default/files/documents/Preliminary-Transcript-CMT-FTC-at-100-2013-12-3.pdf) (accessed Dec. 16, 2013).

Unfairness and even the appearance of unfairness should be avoided by FTC. *Cinderella*,  
425 F.2d at 591; *accord Am. Cyanamid Co.*, 363 F.2d at 767. No FTC official should ever take  
the broad license to prejudge adjudications or to make speeches giving the clear appearance that  
a matter has been decided before a fair evidentiary hearing, as Commissioner Brill has done here.  
*See Cinderella*, 425 F.2d at 589-92. Because Commissioner Brill has “in some measure adjudged  
the facts as well as the law” of LabMD’s case, she must be disqualified. *Id.* at 591.

#### CONCLUSION

For the foregoing reasons, we respectfully move that Commissioner Brill disqualify  
herself immediately and abstain from any further participation in this matter, including, but not  
limited to, participation in the Commission’s forthcoming decision on LabMD’s pending  
Motion to Dismiss.

Respectfully submitted,

/s/ Reed D. Rubinstein  
Reed D. Rubinstein, Partner  
D.C. Bar No. 440153  
William Sherman II, Partner  
D.C. Bar No. 1005932  
Dinsmore & Shohl, L.L.P.  
801 Pennsylvania Ave., NW, Suite 610  
Washington, D.C. 20006  
Telephone: 202.372.9120  
Fax: 202.372.9141  
Email: [reed.rubinstein@dinsmore.com](mailto:reed.rubinstein@dinsmore.com)  
*Counsel to Cause of Action*

PUBLIC



---

Michael D. Pepson  
Cause of Action  
1919 Pennsylvania Ave., NW, Suite 650  
Washington, D.C. 20006  
Phone: 202.499.4232  
Fax: 202.330.5842  
Email: [michael.pepson@causeofaction.org](mailto:michael.pepson@causeofaction.org)  
Admitted only in Maryland.  
Practice limited to cases in federal court and  
administrative proceedings before federal agencies

Dated: December 17, 2013

# **EXHIBIT A**

**Forum Europe Fourth Annual EU Data Protection and Privacy Conference**  
**Commissioner Julie Brill's Keynote Address**  
**September 17, 2013**  
**Brussels, Belgium**

Good morning. I would like to thank Forum Europe for the invitation to participate in this important conference today. I am always delighted to have the opportunity to engage with my EU counterparts on issues that are important to all of us, and I see many of my friends in the audience today.

A lot has changed since this past April when I was last in Brussels. The revelations about the U.S. National Security Agency's programs<sup>1</sup> have sparked a global debate about government surveillance and its effect on individual privacy. As many of you know, I have spent a lifetime working on consumer protection and privacy issues, so it should be no surprise that this is a debate I welcome. It is a conversation that is long overdue, but I also think it is important that we have the right conversation—one that is open and honest, practical and productive. As we move forward with this conversation, my personal view is that there are some important facts that we should keep in mind as we collectively attempt to answer some very tough questions:

- First, whether we call privacy a “fundamental right” or a Constitutional right, the U.S., EU, and many other countries around the world place tremendous value on privacy. Our legislative and regulatory frameworks may differ, but the acknowledgment of the need for privacy protections and the principles underlying how we define those protections are, at their core, the same.<sup>2</sup>
- Second, national security exceptions in laws, including privacy laws, are the norm, not the exception, for countries around the globe, including EU Member States and third countries that have received European Commission adequacy determinations.<sup>3</sup> As we revisit the proper scope of government surveillance, the

---

<sup>1</sup> See Glen Greenwald, Ewen MacAskill & Laura Poitras, *Edward Snowden: the Whistleblower Behind the NSA Surveillance Revelations*, THE GUARDIAN (Jun. 9, 2013), available at <http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance>.

<sup>2</sup> See Julie Brill, Commissioner, Fed. Trade Comm'n, Address at the Mentor Group Forum for EU-US Legal Economic Affairs: Remarks to the Mentor Group (Apr. 16, 2013), available at <http://www.ftc.gov/speeches/brill/130416mentorgroup.pdf>.

<sup>3</sup> See, e.g., Directive 1995/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 2005 O.J. (L 281) 31, 42, available at [http://ec.europa.eu/justice/policies/privacy/docs/95-46-dir1995-46\\_part1\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/95-46-dir1995-46_part1_en.pdf) [hereinafter “EU Data Protection Directive”]; Personal Information Protection and Electronic Documents Act, R.S.C. 2000, c. 5, 6-8, 11, available at <http://laws-lois.justice.gc.ca/PDF/P-8.6.pdf> (Can.). See generally Christopher Wolf, *An Analysis of Service Provider Transparency Reports on Government Requests for Data*, HOGAN LOVELLS (Aug. 27, 2013), <http://www.hldataprotection.com/files/2013/08/Hogan-Lovells-White-Paper-Analysis-of-Transparency-Reports.pdf>.

sufficiency of procedural safeguards, and how to “balance the ends with the means”,<sup>4</sup> we should examine these issues with a global lens, as these challenges are not unique to a single sovereign.

- Third, the recent events provide a teachable moment that should encourage us to redouble our efforts on improving transparency and privacy protections for consumers in the commercial sphere. We have a renewed opportunity to be proactive rather than reactive, and to move the separate but equally important conversation about enhancing consumer privacy forward, not backward. It is important to acknowledge that commercial privacy and national security issues are two distinctly separate issues. Indeed, the EU has recognized this distinction, as the data protection laws do not apply to national security issues.<sup>5</sup> And this is the right approach, helping to ensure the solutions we develop will be tailored to each set of problems we seek to address.

At the Federal Trade Commission, we address commercial privacy. We do not have criminal jurisdiction, or jurisdiction over national security issues. Of course, there are other U.S. officials who are charged with addressing those issues, and they are eager to do so.

The FTC has a long tradition of using its authority against unfair or deceptive practices to protect consumer privacy. We take action against companies that fail to comply with their own privacy policies or otherwise misrepresent their information management practices. And, just as importantly, we also address unfair collection and use of personal information that inflicts harm on consumers that they cannot reasonably avoid, and that does not offer offsetting benefits to consumers or competition.<sup>6</sup>

As specific privacy and data security issues have arisen over the past 40 years, Congress has supplemented the FTC’s broad remedial authority by charging us and other agencies with enforcing other privacy laws, including laws designed to protect financial<sup>7</sup> and health information,<sup>8</sup> children,<sup>9</sup> and information used for credit, insurance, employment and housing decisions.<sup>10</sup>

---

<sup>4</sup> *Full Transcript: President Obama’s Press Conference with Swedish Prime Minister Fredrik Reinfeldt in Stockholm*, WASH. POST, Sept. 4, 2013, available at [http://www.washingtonpost.com/politics/full-transcript-president-obamas-press-conference-with-swedish-prime-minister-fredrik-reinfeldt-in-stockholm/2013/09/04/35e3e08e-1569-11e3-804b-d3a1a3a18f2c\\_story.html](http://www.washingtonpost.com/politics/full-transcript-president-obamas-press-conference-with-swedish-prime-minister-fredrik-reinfeldt-in-stockholm/2013/09/04/35e3e08e-1569-11e3-804b-d3a1a3a18f2c_story.html).

<sup>5</sup> See EU Data Protection Directive, *supra* note 3, at 42.

<sup>6</sup> 15 U.S.C. § 45(n).

<sup>7</sup> Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (codified in scattered sections of 12 and 15 U.S.C.); Fair Credit Reporting Act of 1970 (FRCA), Pub. L. No. 91-508, 84 Stat. 1128 (codified as amended at 15 U.S.C. §§ 1681-1681u).

<sup>8</sup> Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29 & 42 U.S.C.); Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, 42 U.S.C. §§ 201 note, 300jj *et seq.*, 17901.

At the FTC, protecting consumer privacy is one of our most important missions. We have used our broad enforcement authority to challenge inappropriate privacy and data security practices of companies that operate throughout the Internet and mobile ecosystem. Our most well-known cases – against Google,<sup>11</sup> Facebook,<sup>12</sup> and MySpace<sup>13</sup> – have led to orders that, for the next 20 years, govern the data collection and use activities of these companies. And in each of these cases we have addressed the companies’ failure to comply with the U.S.-EU Safe Harbor.

We have also brought myriad cases against companies that are not household names, but whose practices crossed the line. We’ve sued companies spamming consumers and installing spyware on their computers.<sup>14</sup> We’ve challenged companies that failed to properly secure consumer information.<sup>15</sup> We have sued ad networks,<sup>16</sup> analytics companies,<sup>17</sup> data brokers,<sup>18</sup> and software developers.<sup>19</sup> We have vigorously

---

<sup>9</sup> Children’s Online Privacy Protection Act of 1998 (COPPA), Pub. L. 105-277, 112 Stat. 2581-728 (codified as amended at 15 U.S.C. §§ 6501-6505).

<sup>10</sup> 15 U.S.C. §§ 1681-1681t.

<sup>11</sup> In the Matter of Google, Inc., FTC File No. 102 3136 (Oct. 13, 2011), *available at* <http://ftc.gov/os/caselist/1023136/111024googlebuzzdo.pdf> (decision and order).

<sup>12</sup> In the Matter of Facebook, Inc., FTC File No. 092 3184 (July 27, 2012), *available at* <http://www.ftc.gov/os/caselist/0923184/120810facebookdo.pdf> (decision and order).

<sup>13</sup> In the Matter of Myspace, LLC, FTC File No. 102 3058 (Aug. 30, 2012) *available at* <http://ftc.gov/os/caselist/1023058/120911myspacedo.pdf> (decision and order).

<sup>14</sup> *See, e.g., FTC v. Flora*, 2011 U.S. Dist. LEXIS 121712 (C.D. Cal. Aug. 12, 2011), *available at* <http://www.ftc.gov/os/caselist/1023005/110929loanmodorder.pdf>; *FTC v. CyberSpy Software, LLC, et al.*, No. 08-CV-01872 (M.D. Fla. Apr. 22, 2010), *available at* <http://www.ftc.gov/os/caselist/0823160/100602cyberspystip.pdf> (stipulated final order).

<sup>15</sup> *See, e.g., In the Matter of LabMD*, FTC File No. 102 3099 (Aug. 28, 2013), *available at* <http://www.ftc.gov/os/adjpro/d9357/130829labmdpart3.pdf> (administrative complaint).

<sup>16</sup> *See, e.g., In the Matter of Epic Marketplace, Inc. et al.*, FTC File No. 112 3182 (Mar. 13, 2013), *available at* <http://www.ftc.gov/os/caselist/1123182/130315epicmarketplacedo.pdf> (decision and order).

<sup>17</sup> *See, e.g., In the Matter of Upromise, Inc.*, FTC File No. 102 3116 (Apr. 3, 2012), *available at* <http://www.ftc.gov/os/caselist/1023116/120403upromisedo.pdf> (decision and order).

<sup>18</sup> *See, e.g., U.S. v. Spokeo, Inc.*, No. 12-CV-05001 (C.D. Cal. June 19, 2012), *available at* <http://ftc.gov/os/caselist/1023163/120612spokeoorder.pdf> (consent decree and order); *In the Matter of Filiquarian Pub. LLC et al.*, FTC File No. 112 3195 (Apr. 30, 2013), *available at* <http://www.ftc.gov/os/caselist/1123195/130501filquariando.pdf> (decision and order).

<sup>19</sup> *See, e.g., In the Matter of DesignerWare LLC*, FTC File No. 112 3151 (Apr. 11, 2013), *available at* <http://www.ftc.gov/os/caselist/1123151/designerware/130415designerwaredo.pdf> (decision and order).

enforced the Children's Online Privacy Protection Act.<sup>20</sup> And with the world moving to mobile, we have targeted app developers as well as handheld device manufacturers engaged in inappropriate data collection and use practices.<sup>21</sup>

As part of our ongoing effort to address privacy issues in the changing technological landscape, just two weeks ago we brought our first action involving the Internet of Things.<sup>22</sup> In that case, the company failed to secure the software for its Internet-accessible video cameras, which put hundreds of private lives on public display.<sup>23</sup>

Together, these enforcement efforts have established what some scholars call “the common law of privacy” in the United States, in which the FTC articulates – to industry, defense counsel, consumer groups and other stakeholders – in an incremental, but no less effective way, the privacy practices that are deceptive or unfair.<sup>24</sup>

In addition to our privacy enforcement work, the FTC is actively engaged in ongoing policy development to improve privacy protection in light of rapid technological change. We have held hearings and issued reports on cutting edge issues, including facial recognition technology<sup>25</sup>, kids apps,<sup>26</sup> mobile privacy disclosures,<sup>27</sup> and mobile

---

<sup>20</sup> See, e.g., *U.S. v. Path, Inc.*, No. 13-CV-0448 (N.D. Cal. Feb. 8, 2013) (Consent decree and order), available at <http://www.ftc.gov/os/caselist/1223158/130201pathincdo.pdf>.

<sup>21</sup> See, e.g., *In the Matter of HTC, Inc.*, FTC File No. 122 3049 (June 25, 2013), available at <http://www.ftc.gov/os/caselist/1223049/130702htcdo.pdf> (decision and order).

<sup>22</sup> *In the Matter of TRENDnet, Inc.*, FTC File No. 122 3090 (Sept. 4, 2013), available at <http://www.ftc.gov/os/caselist/1223090/130903trendnetorder.pdf> (agreement containing consent order); see also Julie Brill, Op-Ed., *From Regulators, Guidance and Enforcement*, N.Y. TIMES, Sept. 8, 2013, available at <http://www.nytimes.com/roomfordebate/2013/09/08/privacy-and-the-internet-of-things/regulators-must-guide-the-internet-of-things>.

<sup>23</sup> See *id.*

<sup>24</sup> Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. (forthcoming 2014), available at <http://ssrn.com/abstract=2312913>. See also Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247 (2011), (discussing how chief privacy officers reported that “state-of-the-art privacy practices” need to reflect both established black letter law and FTC cases and best practices, including FTC enforcement actions and FTC guidance); Christopher Wolf, *Targeted Enforcement and Shared Lawmaking Authority As Catalysts for Data Protection in the United States*, BNA Privacy and Security Law Report, Oct. 25, 2010, available at [http://www.justice.gov.il/NR/rdonlyres/8D438C53-82C8-4F25-99F8-E3039D40E4E4/26451/Consumer\\_WOLFDataProtectionandPrivacyCommissioners.pdf](http://www.justice.gov.il/NR/rdonlyres/8D438C53-82C8-4F25-99F8-E3039D40E4E4/26451/Consumer_WOLFDataProtectionandPrivacyCommissioners.pdf) (FTC consent decrees have “created a ‘common law of consent decrees,’ producing a set of data protection rules for businesses to follow”).

<sup>25</sup> See Press Release, FTC Recommends Best Practices for Companies That Use Facial Recognition Technologies (Oct. 22, 2012), available at <http://ftc.gov/opa/2012/10/facialrecognition.shtm>.

<sup>26</sup> See FED. TRADE COMM’N, *Mobile Apps for Kids: Disclosures Still Not Making the Grade* (December 2012), available at <http://www.ftc.gov/os/2012/12/121210mobilekidsappreport.pdf>.

payments.<sup>28</sup> Last year the FTC issued its landmark privacy report in which the agency developed a new framework for addressing privacy in the U.S., including best practices for companies to follow based on three core principles: privacy by design, simplified choice, and greater transparency around data collection and use.<sup>29</sup> We called on companies to operationalize the report's recommendations by developing better just-in-time notices and robust choice mechanisms, particularly for health and other sensitive information.<sup>30</sup>

The FTC is also actively studying the data broker industry to learn more about the ways that companies collect, buy, and sell consumer data. We hope to issue a report later this year on how data brokers could improve their privacy practices.<sup>31</sup> In last year's privacy report, the FTC called on Congress to enact data broker legislation that would increase the transparency of the practices of data brokers.<sup>32</sup>

But we don't have to wait for legislation. I recently launched "Reclaim Your Name", a comprehensive initiative to give consumers the means they need to reassert control over their personal data.<sup>33</sup> I call on industry to develop a user-friendly, one-stop online shop to provide consumers with some tools to find out about data broker practices and to exercise reasonable choices about them.<sup>34</sup> Acxiom, the largest data broker in the U.S., has taken the first step toward greater transparency by launching [aboutthedata.com](http://aboutthedata.com), a web portal that allows consumers to access, correct, and suppress the data that the company maintains about them.<sup>35</sup> And while there is certainly room for Acxiom to

---

<sup>27</sup> See Press Release, FTC Staff Report Recommends Ways to Improve Mobile Privacy Disclosures (Feb. 1, 2013), available at <http://www.ftc.gov/opa/2013/02/mobileprivacy.shtm>.

<sup>28</sup> See FED. TRADE COMM'N, *Plastic, Paper, or Mobile? An FTC Workshop on Mobile Payments* (March 2013), available at <http://www.ftc.gov/os/2013/03/130306mobilereport.pdf>.

<sup>29</sup> See FED. TRADE COMM'N, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Mar. 26, 2012) available at <http://www.ftc.gov/os/2012/03/120326privacyreport.pdf> [hereinafter "FTC Privacy Report"].

<sup>30</sup> See *id.*

<sup>31</sup> See Press Release, FTC to Study Data Broker Industry's Collection and Use of Consumer Data (Dec. 12, 2012), available at <http://www.ftc.gov/opa/2012/12/databrokers.shtm>.

<sup>32</sup> See FTC Privacy Report, *supra* note 29, at 14.

<sup>33</sup> See Julie Brill, Commissioner, Fed. Trade Comm'n, Keynote Address at 23<sup>rd</sup> Computers Freedom and Privacy Conference: Reclaim Your Name (June 26, 2013), available at <http://www.ftc.gov/speeches/brill/130626computersfreedom.pdf>.

<sup>34</sup> See *id.* See also Julie Brill, Op-Ed., *Demanding Transparency from Data Brokers*, WASH. POST, Aug. 15, 2013, available at [http://articles.washingtonpost.com/2013-08-15/opinions/41412540\\_1\\_data-brokers-fair-credit-reporting-act-data-fuel](http://articles.washingtonpost.com/2013-08-15/opinions/41412540_1_data-brokers-fair-credit-reporting-act-data-fuel).

<sup>35</sup> See generally Natasha Singer, Acxiom Lets Consumers See Data It Collects, N.Y. TIMES, Sept. 4, 2013, available at <http://www.nytimes.com/2013/09/05/technology/acxiom-lets-consumers-see-data-it-collects.html?pagewanted=all>.

improve its portal, I encourage other industry players to join Acxiom and step up to the plate to provide consumers with greater transparency about their data collection and use practices.

The FTC has also supported baseline privacy legislation.<sup>36</sup> The Obama Administration has been actively working on privacy legislation that would implement its Consumer Privacy Bill of Rights.<sup>37</sup>

Through the FTC Act and other US privacy and data protection laws, the FTC's privacy report and other policy initiatives, and the Obama Administration's Consumer Privacy Bill of Rights, the US aims to achieve many of the same objectives that are outlined in the draft EU data protection regulation. For instance, on both sides of the Atlantic, we are striving to protect children's privacy; spur companies to implement privacy by design, increase transparency, and adopt accountability measures; and require companies to provide notice about data breaches. As the technological challenges facing the EU and the US have grown, so has our common ground in protecting consumers. In some instances, we differ on how to achieve these common goals. For example, we both believe that consumer consent is important, but we have different approaches as to when and how that consent should be obtained. The particular solutions we develop may differ, but the challenges we face and our desire to solve them are the same.

In a world with diverse privacy frameworks, interoperability is critical. We should work together to preserve existing mechanisms and develop new ways that allow our different privacy frameworks to co-exist while facilitating the flow of data across borders. The U.S.-EU Safe Harbor Framework, which enables the lawful transfer of personal data from the EU to the U.S., is vital to preserving interoperability.<sup>38</sup>

Most importantly from my perspective, the Safe Harbor provides the FTC with an effective tool to protect the privacy of EU citizens. Our cases against Google, Facebook, and MySpace — which each protect EU consumers as well as American consumers, and together protect 1 billion consumers worldwide — have demonstrated the effectiveness of this Framework, as well as the FTC's determination to enforce it.

In recent months, the NSA revelations have led some to ask whether the Safe Harbor can adequately protect EU citizens' data in the commercial context. My unequivocal answer to this question is "yes." As I said before, the issue of the proper scope of government surveillance is a conversation that should happen — and will happen — on both sides of the Atlantic. But it is a conversation that should proceed outside out of the

---

<sup>36</sup> See FTC Privacy Report, *supra* note 29, at 13.

<sup>37</sup> See WHITE HOUSE, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (Feb. 23, 2012), available at <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf>.

<sup>38</sup> See U.S. DEP'T OF COMMERCE, *Safe Harbor Privacy Principles* (Jul. 21, 2000), available at [http://export.gov/safeharbor/eu/eg\\_main\\_018475.asp](http://export.gov/safeharbor/eu/eg_main_018475.asp).

commercial privacy context. In the commercial space, the Safe Harbor Framework facilitates the FTC's ability to protect the privacy of EU consumers. Without the Safe Harbor, my job to protect EU consumers' privacy, where appropriate, would be much harder. In an era where we face many threats to privacy, Safe Harbor has been an effective solution, not the problem.

I understand that Safe Harbor, in part because of its notoriety, is an easy target, but I ask you to consider whether it is the right target. Neither the Safe Harbor nor the EU data protection directive was designed to address national security issues.<sup>39</sup> Data transferred to "adequate" countries, or through binding corporate rules, approved contractual clauses, or the Safe Harbor, are all subject to the same national security exceptions. The most salient difference is that, for transfers made pursuant to Safe Harbor, the FTC is the cop on the beat for commercial privacy issues. The same is not true of the other transfer mechanisms. So, from my consumer protection enforcer's perspective, the Safe Harbor provides more, not less, privacy protection. And, for that reason, I support its continuation.

While some things have changed since my last trip to Brussels in April, many things have remained the same. Our enforcement is still robust, including our enforcement of the Safe Harbor. Our policy development continues. And I believe that the common ground between the U.S. and the EU is still quite fertile.

Last April when I was here I quoted one of my heroes, John F. Kennedy, and I believe it is worth quoting him again. Fifty years ago, in 1963, he said: "[L]et us not be blind to our differences—but let us also direct attention to our common interests and to the means by which those differences can be resolved. And if we cannot end now our differences, at least we can help make the world safe for diversity."<sup>40</sup>

These words continue to ring true – especially now, when we each have so much work to do to foster better consumer privacy protections for all of our citizens.

---

<sup>39</sup> See *id.* See also EU Data Protection Directive, *supra* note 3.

<sup>40</sup> See John F. Kennedy, Commencement Address at American University: Towards a Strategy of Peace (June 10, 1963), available at <http://www.jfklibrary.org/Asset-Viewer/BWC714C9QUmLG9J618oy8w.aspx>.

# **EXHIBIT B**

**Commissioner Julie Brill's Opening Panel Remarks**  
**European Institute**  
**Data Protection, Privacy and Security:**  
**Re-Establishing Trust Between Europe and the United States**  
**October 29, 2013**

Good morning. I would like to thank Joëlle Attinger and the European Institute for inviting me to speak to you today. I am honored to be here with Jan Philipp Albrecht, Jim Halpert, and our esteemed colleagues from the European Parliament's LIBE committee. Welcome to Washington. I am very happy to say that we are once again open for business.

Your visit comes on the heels of a significant milestone in Brussels. Just last week, the LIBE committee reconciled thousands of amendments to the proposed EU data protection legislation, passed an initial draft, and authorized negotiations with the Council.<sup>1</sup>

In the U.S., we have followed the EU's revision of its privacy framework closely. Although we often hear about the differences between the U.S. and EU privacy frameworks, I think it's important to highlight that we share many of the same goals. The draft EU data protection legislation that the LIBE committee approved last week adopts measures that echo many of the FTC's efforts here in the U.S., including calling on firms to:

- Adopt privacy by design;
- Increase transparency;
- Enhance consumer control;
- Improve data accuracy and consumers' access to their data;
- Strengthen data security;
- Provide parental control over information companies collect about children; and
- Encourage accountability.<sup>2</sup>

As the technological challenges facing the EU and the U.S. have grown, so has our common effort to protect consumers. In some cases, we differ on how to achieve these common goals.<sup>3</sup> For example, we both believe that consent is important, but we have different approaches

---

<sup>1</sup> See Press Release, European Parliament Committee on Civil Liberties, Justice, and Home Affairs, Civil Liberties MEPs pave the way for stronger data protection in the EU (Oct. 21, 2013), available at <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fTEXT%2bIM-PRESS%2b20131021IPR22706%2b0%2bDOC%2bXML%2bV0%2f%2fEN&language=EN>.

<sup>2</sup> See Commission Proposal for a Directive of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation), COM (2012) 11 amended (Oct. 21, 2013), available at [http://www.europarl.europa.eu/meetdocs/2009\\_2014/documents/libe/dv/comp\\_am\\_art\\_01-29/comp\\_am\\_art\\_01-29en.pdf](http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/comp_am_art_01-29/comp_am_art_01-29en.pdf), [http://www.europarl.europa.eu/meetdocs/2009\\_2014/documents/libe/dv/comp\\_am\\_art\\_30-91/comp\\_am\\_art\\_30-91en.pdf](http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/comp_am_art_30-91/comp_am_art_30-91en.pdf) (listing the European Parliament Committee on Civil Liberties, Justice, and Home Affairs's latest amendments to Articles 1-91); FED. TRADE COMM'N, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Mar. 26, 2012), available at <http://www.ftc.gov/os/2012/03/120326privacyreport.pdf>.

as to when and how that consent should be obtained. The particular means we choose may differ, but the challenges we face and our focus on solving them are the same.

Despite our commonalities, recent events make the title of today's discussion – “Re-Establishing Trust Between Europe and the United States” – particularly relevant. There is no doubt that the revelations about the National Security Agency's surveillance programs have severely tested the close friendship between the US and many of our European colleagues. Let me take a moment to address this issue.

Edward Snowden's disclosures about the NSA have sparked a global debate about government surveillance and its impact on individual privacy.<sup>4</sup> There is great interest in the United States and in Europe in having the revelations about the NSA serve as a catalyst for change in the way governments engage in surveillance to enhance national security. As some of you know, I have spent a lifetime working on privacy issues, so it should be no surprise that this is a debate I personally welcome, as my own view is that it is a conversation that is overdue.

But I also think it is important that we have the right conversation — one that is open and honest, practical and productive. As we move forward with this conversation, we should keep in mind that consumer privacy in the commercial sphere, and citizens' privacy in the face of government surveillance to protect national security, are two distinctly separate issues. I and my colleagues at the FTC focus on the appropriate balance between consumer privacy interests and commercial firms' use of consumer data, not on national security issues. And I believe the recent revelations should spur a separate and equally long overdue conversation about how we can further enhance consumer privacy and increase transparency in the commercial sphere.

The FTC is the premier U.S. consumer protection agency focused on commercial privacy. The FTC has a great track record of using its authority to go after unfair or deceptive practices that violate consumer privacy, and vigorously enforcing other laws designed to protect financial<sup>5</sup> and health<sup>6</sup> information, information about children<sup>7</sup>, and credit information used to make decisions about credit, insurance, employment, and housing.<sup>8</sup>

---

<sup>3</sup> See Julie Brill, Commissioner, Fed. Trade Comm'n, Address at the Mentor Group Forum for EU-US Legal Economic Affairs: Remarks to the Mentor Group (Apr. 16, 2013), available at <http://www.ftc.gov/speeches/brill/130416mentorgroup.pdf>.

<sup>4</sup> See Glen Greenwald, Ewen MacAskill & Laura Poitras, *Edward Snowden: the Whistleblower Behind the NSA Surveillance Revelations*, THE GUARDIAN (JUN. 9, 2013), available at <http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance>.

<sup>5</sup> Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (codified in scattered sections of 12 and 15 U.S.C.).

<sup>6</sup> Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29 & 42 U.S.C.); Health Information Technology for Economic and Clinical Health Act of 2009, 42 U.S.C. 300jj et seq. §§17901 et seq.

<sup>7</sup> Children's Online Privacy Protection Act of 1998, Pub. L. 105-277, 112 Stat. 2581-728 (codified as amended at 15 U.S.C. §§ 6501-6505).

We have used our broad enforcement authority to challenge inappropriate privacy and data security practices of companies that operate throughout the Internet and mobile ecosystem. We have brought enforcement actions against well-known companies, such as Google,<sup>9</sup> Facebook,<sup>10</sup> Twitter,<sup>11</sup> and Myspace.<sup>12</sup>

We have also brought myriad cases against companies that are not household names, but whose practices violated the law. We've sued companies that spammed consumers,<sup>13</sup> installed spyware on computers,<sup>14</sup> failed to secure consumers' personal information,<sup>15</sup> deceptively tracked consumers online,<sup>16</sup> violated children's privacy laws,<sup>17</sup> inappropriately collected information on consumers' mobile devices,<sup>18</sup> and failed to secure Internet-connected devices.<sup>19</sup> We have obtained millions of dollars in penalties and restitution in our privacy and data security cases, and placed numerous companies under 20-year orders with robust injunctive provisions.

---

<sup>8</sup> Fair Credit Reporting Act of 1970, Pub. L. No. 91-508, 84 Stat. 1128 (codified as amended at 15 U.S.C. §§ 1681-1681x).

<sup>9</sup> In the Matter of Google, Inc., FTC File No. 102 3136 (Oct. 13, 2011), *available at* <http://ftc.gov/os/caselist/1023136/111024googlebuzzdo.pdf> (decision and order).

<sup>10</sup> In the Matter of Facebook, Inc., FTC File No. 092 3184 (July 27, 2012), *available at* <http://www.ftc.gov/os/caselist/0923184/120810facebookdo.pdf> (decision and order).

<sup>11</sup> In the Matter of Twitter, Inc., FTC File No. 092 3093 (March 3, 2011) *available at* <http://www.ftc.gov/os/caselist/0923093/110311twitterdo.pdf> (decision and order).

<sup>12</sup> In the Matter of Myspace, LLC, FTC File No. 102 3058 (Aug. 30, 2012) *available at* <http://ftc.gov/os/caselist/1023058/120911myspacedo.pdf> (decision and order).

<sup>13</sup> *See, e.g., FTC v. Flora*, 2011 U.S. Dist. LEXIS 121712 (C.D. Cal. Aug. 12, 2011), *available at* <http://www.ftc.gov/os/caselist/1023005/110929loanmodorder.pdf>.

<sup>14</sup> *See, e.g., FTC v. CyberSpy Software, LLC, et al.*, No. 08-CV-01872 (M.D. Fla. Apr. 22, 2010), *available at* <http://www.ftc.gov/os/caselist/0823160/100602cyberspystip.pdf> (stipulated final order).

<sup>15</sup> *See, e.g., In the Matter of LabMD*, FTC File No. 102 3099 (Aug. 28, 2013), *available at* <http://www.ftc.gov/os/adjpro/d9357/130829labmdpart3.pdf> (administrative complaint).

<sup>16</sup> *See, e.g., In the Matter of Epic Marketplace, Inc., et al.*, FTC File No. 112 3182 (Dec. 5, 2012), *available at* <http://www.ftc.gov/os/caselist/1123182/130315epicmarketplacedo.pdf> (decision and order).

<sup>17</sup> *See, e.g., U.S. v. Artist Arena, LLC*, No. 12-CV-7386 (S.D.N.Y. Oct. 3, 2012), *available at* <http://www.ftc.gov/os/caselist/1123167/121003artistarenadecree.pdf> (stipulated final order).

<sup>18</sup> *See U.S. v. Path, Inc.*, No. 13-CV-0448 (N.D. Cal. Feb. 8, 2013) (Consent decree and order), *available at* <http://www.ftc.gov/os/caselist/1223158/130201pathincdo.pdf>; In the Matter of HTC, Inc., FTC File No. 122 3049 (June 25, 2013), *available at* <http://www.ftc.gov/os/caselist/1223049/130702htcdo.pdf> (decision and order).

<sup>19</sup> *See In the Matter of TRENDnet, Inc.*, FTC File No. 122 3090 (Sept. 4, 2013), *available at* <http://www.ftc.gov/os/caselist/1223090/130903trendnetorder.pdf> (agreement containing consent order); *see also* Julie Brill, Op-Ed., *From Regulators, Guidance and Enforcement*, N.Y. TIMES, Sept. 8, 2013, *available at* <http://www.nytimes.com/roomfordebate/2013/09/08/privacy-and-the-internet-of-things/regulators-must-guide-the-internet-of-things>.

As a complement to our privacy enforcement work, the FTC is actively engaged in ongoing policy development to improve privacy protection in light of rapid technological change. In addition to our landmark privacy report issued last year, we have addressed cutting-edge privacy issues involving facial recognition technology,<sup>20</sup> kids apps,<sup>21</sup> mobile privacy disclosures,<sup>22</sup> and mobile payments.<sup>23</sup>

In light of our increasingly interconnected world, the FTC has devoted significant time to enhancing international privacy enforcement cooperation so that we are better able to address global challenges. We continue to foster a strong relationship and engage in ongoing dialogue with European data protection authorities. We meet regularly with EU DPAs, and in April I met with the entire Article 29 Working Party. The Article 29 Working Party has been kind enough to recognize the FTC as a crucial partner in privacy and data protection enforcement.<sup>24</sup> And the Working Party, like the FTC, has welcomed the ongoing dialogue and constructive cooperation between us, and stressed the need for further transatlantic cooperation, especially in enforcement matters, in order to achieve our common goals.<sup>25</sup> Indeed, the FTC's recent Memorandum of Understanding with the Irish DPA establishes a good framework for increased, more streamlined, and more effective privacy enforcement cooperation.<sup>26</sup> And just last month, we worked very closely with our EU and Canadian counterparts to launch the International Conference of Data Protection and Privacy Commissioners' initiative to address challenges in global privacy enforcement cooperation.<sup>27</sup>

---

<sup>20</sup> See Press Release, FTC Recommends Best Practices for Companies That Use Facial Recognition Technologies (Oct. 22, 2012), available at <http://ftc.gov/opa/2012/10/facialrecognition.shtm>.

<sup>21</sup> See FED. TRADE COMM'N, *Mobile Apps for Kids: Disclosures Still Not Making the Grade* (December 2012), available at <http://www.ftc.gov/os/2012/12/121210mobilekidsappreport.pdf>.

<sup>22</sup> See Press Release, FTC Staff Report Recommends Ways to Improve Mobile Privacy Disclosures (Feb. 1, 2013), available at <http://www.ftc.gov/opa/2013/02/mobileprivacy.shtm>.

<sup>23</sup> See FED. TRADE COMM'N, *Plastic, Paper, or Mobile? An FTC Workshop on Mobile Payments* (March 2013), available at <http://www.ftc.gov/os/2013/03/130306mobilereport.pdf>.

<sup>24</sup> Press Release, Article 29 Data Protection Working Party Meeting with FTC Commissioner Julie Brill (Apr. 29, 2013), available at [http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29\\_press\\_material/20130429\\_pr\\_april\\_plenary\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20130429_pr_april_plenary_en.pdf).

<sup>25</sup> See *Id.*

<sup>26</sup> Memorandum of Understanding Regarding Mutual Assistance in the Enforcement of Laws Protecting Personal Information in the Private Sector, U.S. FED. TRADE COMM'N-DATA PROTECTION COMMISSIONER OF IRELAND, June 2013, available at <http://www.ftc.gov/os/2013/06/130627usirelandmouprivacyprotection.pdf>.

<sup>27</sup> See Resolution on International Enforcement and Cooperation, 35th International Conference of Data Protection and Privacy Commissioners, Sept. 23-26, 2013, available at <https://privacyconference2013.org/web/pageFiles/kcfinder/files/4.%20Enforcement%20coordination%20resolution%20EN%20.pdf>.

Another critical role played by the FTC is to enforce the U.S.-EU Safe Harbor framework.<sup>28</sup> We know that Safe Harbor has received its share of criticism, particularly in the past few months. We've read the news reports and heard about the recent Parliamentary hearings about Safe Harbor.<sup>29</sup> Given the active debate over Safe Harbor right now, I'd like to address head-on the contention in some quarters that Safe Harbor isn't up to the job of protecting EU citizens' data in the commercial sphere.

First, the FTC vigorously enforces the Safe Harbor. As the Safe Harbor program has grown over the past decade, so has the FTC's enforcement activity. Since 2009, we have brought ten Safe Harbor cases.<sup>30</sup> When Safe Harbor was established, the FTC committed to review on a priority basis all referrals from EU member state authorities.<sup>31</sup> With few referrals over the past decade, we have taken the initiative to proactively look for Safe Harbor violations in every privacy and data security investigation we conduct. That is how we discovered the Safe Harbor violations of Google, Facebook, and Myspace in the last few years. These cases demonstrate the enforceability of Safe Harbor certifications and the high cost that companies can pay for non-compliance. The orders in Google, Facebook, and Myspace require the companies to implement comprehensive privacy programs and subject the companies to ongoing privacy audits for 20 years.<sup>32</sup> Violations of these orders can result in hefty fines, as Google discovered when we assessed a \$22.5 million civil penalty against the company last year for violating its consent decree.<sup>33</sup> The FTC orders against Google, Facebook, and Myspace help protect over a billion consumers worldwide, hundreds of millions of whom reside in Europe. These cases demonstrate that Safe Harbor gives the FTC an effective and functioning tool to protect the privacy of EU citizen data transferred to America. Without the Safe Harbor, my job to protect EU consumers' privacy, where appropriate, would be much harder. In an era where we face many threats to privacy, Safe Harbor has been an effective solution, not the problem.

Second, going forward, the FTC will continue to make the Safe Harbor a top enforcement priority. Indeed, we have opened numerous investigations into Safe Harbor compliance in recent months. We will continue to welcome any substantive leads, such as the complaint we received in the past month from a European-based consumer advocate alleging a large number of Safe Harbor-related violations. And, let me be clear, we take this recent complaint very seriously. Of

---

<sup>28</sup> See U.S. DEP'T OF COMMERCE, *Safe Harbor Privacy Principles* (Jul. 21, 2000), available at [http://export.gov/safeharbor/eu/eg\\_main\\_018475.asp](http://export.gov/safeharbor/eu/eg_main_018475.asp).

<sup>29</sup> See LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens, Sixth Hearing (Oct. 7, 2013), available at <http://www.europarl.europa.eu/ep-live/en/committees/video?event=20131014-1500-COMMITTEE-LIBE>.

<sup>30</sup> See Legal Resources, Bureau of Consumer Protection Business Center, U.S. FED. TRADE COMM'N, available at <http://business.ftc.gov/legal-resources/2840/3>.

<sup>31</sup> See Letter from Robert Pitofsky, Chairman, Fed. Trade Comm'n to John Mogg, Director, Directorate-General XV, European Commission (Jul. 14, 2000), available at [http://export.gov/static/sh\\_en FTCLETTERFINAL Latest eg\\_main\\_018455.pdf](http://export.gov/static/sh_en FTCLETTERFINAL Latest eg_main_018455.pdf).

<sup>32</sup> See Google, *supra* note 9; Facebook, *supra* note 10; Myspace, *supra* note 12.

<sup>33</sup> See 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 <http://ftc.gov/opa/2012/08/google.shtm>.

course, as we do in every instance, we take the necessary time to separate fact from fiction. And, as I am sure many in this audience would appreciate, we also proceed carefully to provide proper notice and appropriate levels of due process. If we discover in our investigations that companies have committed Safe Harbor-related law violations, we will take appropriate enforcement actions.

As I mentioned earlier, I think it is healthy to have a vigorous debate over how to appropriately balance national security and privacy, but that ongoing debate should not be allowed to distort discussions in the commercial sphere about role of the Safe Harbor in protection consumer privacy. The EU itself has created national security exemptions in its existing data protection laws,<sup>34</sup> and the European Commission proposed such exemptions for government surveillance in its draft data protection regulation.<sup>35</sup> In other words, the EU has justifiably recognized the need to tackle their member states' national security issues separately. Safe Harbor is no different and warrants a similar approach. Just as the EU Data Protection Directive was not designed to address national security issues, neither was the Safe Harbor. Whatever the means to transfer data about European consumers for commercial purposes – whether to countries whose laws are deemed “adequate”, through approved contractual clauses, or by way of the Safe Harbor – all these transfer mechanisms are subject to national security exceptions. The difference is that, for Safe Harbor violations, the FTC is the cop on the beat. So, from my consumer protection enforcer's perspective, the Safe Harbor provides more, not less, privacy protection.

I know that some of you in this room may have taken a different view of the Safe Harbor framework. I hope my thoughts give you cause to reexamine the virtues of the Safe Harbor system. As the draft regulation continues its journey through the process of review and adoption, I am hopeful that we can continue to work together to promote both the free flow of data and strong consumer privacy protections.

And while it may not make the headlines or the nightly news, in the midst of all of the recent developments at home and across the pond, our efforts to enhance privacy enforcement cooperation continue to build trust day by day. We want to continue to develop these ties of cross border law enforcement cooperation – including Safe Harbor enforcement – that enhance privacy and data security – as these are the ties that build rather than erode trust, the ties that bind rather than divide us. We have worked extensively with our friends in the EU on these and other issues, and we look forward to continuing that collaboration to enhance privacy protection for consumers on both sides of the Atlantic.

Thank you.

---

<sup>34</sup> Directive 1995/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 2005 O.J. (L 281) 31, 42, available at [http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46\\_part1\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf).

<sup>35</sup> See Commission Proposal for a Directive of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation), COM (2012) 11 final (Jan. 25, 2012), available at [http://ec.europa.eu/justice/data-protection/document/review2012/com\\_2012\\_11\\_en.pdf](http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf).



PUBLIC

**CERTIFICATE OF SERVICE**

I hereby certify that on December 17, 2013, I filed the foregoing document electronically using the FTC's E-Filing System, which will send notification of such filing to:

Donald S. Clark, Esq.  
Secretary  
Federal Trade Commission  
600 Pennsylvania Ave., NW, Rm. H-113  
Washington, DC 20580

I certify that I caused hand-delivery of twelve paper copies of the foregoing document to the following address: Document Processing Section, Room H-113, Headquarters Building, 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580.

I also certify that I delivered via electronic mail and caused hand-delivery of a copy of the foregoing document to:

The Honorable D. Michael Chappell  
Chief Administrative Law Judge  
Federal Trade Commission  
600 Pennsylvania Ave., NW, Rm. H-110  
Washington, DC 20580

I further certify that I delivered via electronic mail and first-class mail a copy of the foregoing document to:

Alain Sheer, Esq.  
Laura Riposo VanDruff, Esq.  
Megan Cox, Esq.  
Margaret Lassack, Esq.  
Ryan Mehm, Esq.  
John Krebs, Esq.  
Division of Privacy and Identity Protection  
Federal Trade Commission  
600 Pennsylvania Ave., N.W.  
Mail Stop NJ-8122  
Washington, D.C. 20580

**CERTIFICATE OF ELECTRONIC FILING**

I certify that the electronic copy sent to the Secretary of the Commission is a true and correct copy of the paper original and that I possess a paper original of the signed document that is available for review by the parties and the adjudicator.

Dated: December 17, 2013

By:   
Michael D. Pepson