**Before the**
**FEDERAL COMMUNICATIONS COMMISSION**
**Washington, DC 20554**

| | | |
|---|---|---|
| In the Matter of | ) | |
| | ) | WC Docket No. 16-106 |
| Protecting the Privacy of Customers of Broadband and Other Telecommunications Services | ) | FCC 16-39 |

To: The Federal Communications Commission
Date: May 27, 2016

**Comment of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission**

## I. INTRODUCTION

The collection, use, and sharing of consumer data drives valuable innovation across many fields – benefiting consumers enormously – but also creates privacy risks. These risks create challenges for consumers and businesses. Consumers may be concerned, for example, about the massive collection and storage of their personal information; the risk that their personal information will fall into the wrong hands, enabling identity theft and other harms; the release of sensitive information they regard as private; and the potential use of certain data by employers, insurers, creditors, and others to make important decisions about them. To the extent that these concerns interfere with consumers' willingness to engage in online transactions, businesses may also be at risk.

Recent surveys demonstrate that concerns about privacy and security are common. For example, the National Telecommunications and Information Association ("NTIA") analyzed recent Census data, and found that 84% of surveyed online households expressed at least one

concern about online privacy or security.[1] Forty-five percent of surveyed online households reported that these concerns stopped them from some online activities, such as conducting financial transactions, buying goods or services, posting on social networks, or expressing opinions on controversial or political issues via the Internet.[2] As this data shows, while consumers continue to increase their online presence,[3] privacy and security are important not just for consumers but is also a crucial component for building trust in the online marketplace.

Recognizing the importance of protecting consumer privacy, the Federal Communications Commission ("FCC") issued a Notice of Proposed Rulemaking on Protecting the Privacy of Customers of Broadband and Other Telecommunications Services ("Privacy NPRM" or "NPRM").[4] The NPRM addresses Broadband Internet Access Service ("BIAS"), which the FCC reclassified as a common carrier service in 2015.[5] The FCC's NPRM seeks comment on proposed rules governing the privacy of consumer information collected by

[1] Rafi Goldberg, *Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities*, NTIA (May 13, 2016), *available at* https://www.ntia.doc.gov/print/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities.
[2] *Id.*
[3] *See, e.g.*, *Andrew Perrin, Social Media Usage: 2005-2015*, Pew Research Center, *available at* http://www.pewinternet.org/2015/10/08/social-networking-usage-2005-2015/ (discussing how nearly two-thirds of all American adults used social networking sites in 2015, up from 7% in 2005).
[4] Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, Notice of Proposed Rulemaking, WC Docket No. 16-106, FCC 16-39 (released Apr. 1, 2016), *published in* 81 Fed. Reg. 23360 (April 20, 2016) ("Privacy NPRM").
[5] Because the FTC Act excepts common carrier activities from the FTC's jurisdiction, the FCC's action had the effect of removing BIAS services from the FTC's jurisdiction.

broadband Internet access services providers ("BIAS providers").[6] The proposed rules are intended to promote transparency, consumer choice, and security. The Federal Trade Commission's Staff of the Bureau of Consumer Protection ("FTC staff") commends the FCC for its attention to these issues and provides the following comments, based on the FTC's decades of experience pursuing law enforcement, consumer and business education, and policy activities, described below.

## II. THE FTC'S PRIVACY PROGRAM

As part of its consumer protection mandate, the FTC enforces a wide range of laws to protect the privacy and security of consumer data. The primary law enforced by the FTC, the FTC Act, prohibits "unfair" and "deceptive" acts or practices in or affecting commerce.[7] A misrepresentation or omission is deceptive if it is material and is likely to mislead consumers acting reasonably under the circumstances.[8] An act or practice is unfair if it causes, or is likely to cause, substantial injury that is not reasonably avoidable by consumers, and not outweighed by countervailing benefits to consumers or competition.[9] The FTC also enforces sector-specific

[6] Title II and its implementing rules apply to telecommunications carriers "only to the extent that [they are] engaged in providing telecommunications services." 47 U.S.C. § 153(51); *see also* 47 U.S.C. § 332(c)(1)(A), (c)(2). The FCC's order reclassifying BIAS as common carriage unequivocally applied the same principle *See Protecting and Promoting the Open Internet*, 30 FCC 5601, 5682-83, ¶¶ 187-88 (2015); 47 C.F.R. § 8.11(a). The text of the NPRM makes clear that a similar definition is intended here. *See, e.g.*, NPRM, ¶¶ 9, 11, 53-55. FTC staff recommends that the FCC clarify this principle in its final report and order and adopt a corresponding definition of Broadband Internet Access Service Provider in the rule. For example, Proposed Rule § 64.7000(d) could be modified as follows by adding the terms shown in italics: "The term 'broadband Internet access provider' or 'BIAS provider' means a person or entity ***to the extent that it is*** engaged in the provision of BIAS." In addition, as both the FTC and FCC agree, the common carrier exception applies only to actual common carrier services. FCC-FTC Consumer Protection Memorandum of Understanding, at 2 (2015), *available at* https://www ftc.gov/policy/cooperation-agreements/memorandum-understanding-consumer-protection-between-federal-trade. We recommend that the FCC, in its final report and order, clarify the language in ¶ 288 of the NPRM.

[7] 15 U.S.C. § 45(a).

[8] *See* FTC Policy Statement on Deception, *appended to Cliffdale Assocs., Inc.*, 103 F.T.C. 110, 174 (1984), *available at* https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception.

[9] *See* FTC Policy Statement on Unfairness, *appended to Int'l Harvester Co.*, 104 F.T.C. 949, 1070 (1984), *available at* https://www ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness; 15 U.S.C. §45(n).

statutes that protect certain health, credit, financial, and children's information, and has issued regulations implementing each of these statutes.[10]

Enforcement is the lynchpin of the FTC's approach to privacy protection. To date, the FTC has brought over 500 cases protecting the privacy and security of consumer information.[11] This body of cases covers both offline and online information and includes enforcement actions against companies large and small. In a wide range of cases, the FTC has alleged that companies made deceptive claims about how they collect, use, and share consumer data;[12] failed to provide reasonable security for consumer data;[13] deceptively tracked consumers online;[14] spammed and defrauded consumers;[15] installed spyware or other malware on consumers' computers;[16] violated Do Not Call and other telemarketing rules;[17] shared highly sensitive, private consumer data with

[10] *See, e.g.*, Health Breach Notification Rule, 16 C.F.R. Part 318 *et seq.*, effectuating 42 U.S.C. § 17937(g) (notification for breach of health information); Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq*.; Gramm-Leach-Bliley Act Safeguards Rule, 16 C.F.R. Part 314 *et seq*. (financial information security); Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6501 *et seq*. and 16 C.F.R. Part 412 (children's online information security and privacy).

[11] Letter from Edith Ramirez, Chairwoman, Fed Trade Comm'n, to Věra Jourová, Commissioner for Justice, Consumers, and Gender Equality, European Commission, at 3 (Feb. 23, 2016), *available at* https://www.ftc.gov/public-statements/2016/02/letter-chairwoman-edith-ramirez-vera-jourova-commissioner-justice.

[12] *See, e.g.*, Snapchat, Inc., Docket No. C-4501 (Dec. 23, 2014) (decision and order), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3078/snapchat-inc-matter; *see generally* FTC, Privacy and Security Cases, https://www.ftc.gov/datasecurity.

[13] *See, e.g.*, Accretive Health, Inc., Docket No. C-4432 (decision and order) (Feb. 24, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/122-3077/accretive-health-inc-matter; *FTC v. Neovi Inc.*, 604 F.3d 1150 (9th Cir. 2010); *see generally* FTC, Privacy and Security Cases, https://www.ftc.gov/datasecurity.

[14] *See, e.g.*, Compete, Inc., Docket No. C-4384 (Feb. 20, 2013) (decision and order), *available at* https://www.ftc.gov/enforcement/cases-proceedings/102-3116/compete-inc; Upromise, Inc., Docket No. C-4351 (Mar. 27, 2012) (decision and order), *available at* https://www ftc.gov/enforcement/cases-proceedings/102-3116/upromise-inc; Sears Holding Mgt. Corp., Docket No. C-4264 (Aug. 31, 2009) (decision and order), *available at* https://www ftc.gov/enforcement/cases-proceedings/082-3099/sears-holdings-management-corporation-corporation-matter.

[15] *See, e.g.*, *FTC v. INC21.com Corp.*, 688 F. Supp. 2d 927 (N.D. Cal. 2010), *aff'd*, 475 Fed. Appx. 106 (9th Cir. 2012); *see generally* FTC, Online Advertising and Marketing, https://www.ftc.gov/tips-advice/business-center/advertising-and-marketing/online-advertising-and-marketing.

[16] *See generally* FTC Media Resources, Spyware and Malware, *available at* https://www ftc.gov/news-events/media-resources/identity-theft-and-data-security/spyware-and-malware.

[17] *See, e.g.*, *FTC v. E.M.A. Nationwide, Inc.*, 767 F.3d 611 (6th Cir. 2014); *see generally* FTC, Online Advertising and Marketing, https://www.ftc.gov/tips-advice/business-center/advertising-and-marketing/telemarketing.

unauthorized third parties,[18] and publicly posted such data online without consumers' knowledge or consent.[19] The many companies under FTC orders include Microsoft, Facebook, Google, Equifax, HTC, Twitter, Snapchat, and Wyndham Hotels.[20] The FTC's ongoing enforcement actions – in both the physical and digital worlds – send an important message to companies about the need to protect consumers' privacy and data security.

The FTC also has pursued numerous policy initiatives designed to enhance consumer privacy. For example, the FTC has hosted workshops and issued reports to improve privacy disclosures in the mobile ecosystem; increase transparency in the data broker industry; maximize the benefits of big data while mitigating its risks, particularly for low-income and underserved consumers; and highlight the privacy and security implications of facial recognition and the Internet of Things.[21]

Finally, the FTC engages in consumer and business education to increase the impact of its enforcement and policy development initiatives. The FTC uses a variety of tools – brochures, online resources, workshops, and social media – to distribute educational materials on a wide range of topics, including mobile apps, children's privacy, and data security. Most recently on

---

[18] *See, e.g.*, *FTC v. Accusearch, Inc.*, 570 F.3d 1187, 1195 (10th Cir. 2009) (*en banc*).

[19] *See, e.g.*, Jerk, LLC, d/b/a Jerk.com, Docket No. 9361, *available at* https://www ftc.gov/enforcement/cases-proceedings/122-3141/jerk-llc-dba-jerkcom-matter; Craig Brittain, Docket No. C-4564 (Dec. 28, 2015) (decision and order), *available at* https://www ftc.gov/enforcement/cases-proceedings/132-3120/craig-brittain-matter (placing explicit photos of women and girls online without their consent).

[20] *See generally* FTC, Privacy and Security Cases, https://www.ftc.gov/datasecurity.

[21] *See, e.g.*, FTC Staff Report, Mobile Privacy Disclosures: Building Trust Through Transparency (Feb. 2013), *available at* https://www.ftc.gov/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission ("Mobile Disclosures Report"); FTC Report, Data Brokers: A Call for Transparency and Accountability (May 2014), *available at* https://www ftc.gov/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014 ("Data Broker Report"); FTC Staff Report, Internet of Things: Privacy & Security in a Connected World (Jan. 2015) *available at* https://www.ftc.gov/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things ("Internet of Things Report"); FTC Staff Report, Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies (Oct. 2012), *available at* https://www.ftc.gov/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies; *see also* FTC Workshop, Internet of Things: Privacy & Security in a Connected World (Nov. 19, 2013), *available at* https://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices.

the business education front, the FTC launched its "Start with Security" initiative, which includes new guidance for businesses on the lessons learned from the FTC's data security cases, as well as workshops across the country.[22] For consumer education, the FTC recently announced the rollout of its enhanced IdentityTheft.gov website,[23] a free, one-stop resource people can use to report and begin the process of recovery from identity theft. Now, identity theft victims can use the site to create a personal recovery plan based on the type of identity theft they face, and get pre-filled letters and forms to send to credit bureaus, businesses, debt collectors, the IRS, and others.

## III. OVERVIEW OF FTC COMMENTS

As a general matter, FTC staff commends the FCC's focus on transparency, consumer choice, and data security. The FTC's many privacy initiatives have consistently emphasized these core principles. For example, many of the FTC's recent privacy cases have focused on companies' deceptive failure to disclose clearly their information collection, use, and sharing practices.[24] Others have alleged that companies engaged in deceptive practices that undermined

[22] *See generally* Press Release, *FTC Kicks Off "Start with Security" Business Education Initiative* (June 30, 2015), *available at* https://www.ftc.gov/news-events/press-releases/2015/06/ftc-kicks-start-security-business-education-initiative.

[23] *See* Press Release, *FTC Announces Significant Enhancements to IdentityTheft.gov* (Jan. 28, 2016), *available at* https://www.ftc.gov/news-events/press-releases/2016/01/ftc-announces-significant-enhancements-identitytheftgov; *see also* https://robodeidentidad.gov/ in Spanish).

[24] *See, e.g.*, PaymentsMD, LLC, Docket No. C-4505 (Jan. 27, 2015) (decision and order), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3088/paymentsmd-llc-matter (alleging deceptive failure to adequately disclose that company would be seeking consumers' health information from third parties, such as pharmacies); Goldenshores Techs., LLC, Docket No. C-4446 (Mar. 31, 2014) (decision and order), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3087/goldenshores-technologies-llc-erik-m-geidl-matter (alleging deceptive failure to disclose that a flashlight app transmitted geolocation information to third parties); Epic Marketplace, Inc., Docket No. C-4389 (Mar. 13, 2013) (decision and order), *available at* https://www.ftc.gov/enforcement/cases-proceedings/112-3182/epic-marketplace-inc (alleging deceptive failure to disclose that consumers were being tracked through browser history sniffing).

consumers' ability to exercise choices.[25] And to promote strong data security practices, the FTC has brought approximately sixty enforcement actions, launched numerous business education initiatives, and repeatedly advocated for federal legislation that would give the FTC additional tools, and consumers additional protections, in this area.[26]

This comment provides FTC staff's views on all three issues: transparency, choice, and security. Many of these recommendations are interdependent.[27] On transparency, the NPRM would require a BIAS provider to "clearly and conspicuously notify its customers of its privacy policies," and sets forth requirements for the content of the policies.[28] As discussed below, FTC staff generally supports the proposed transparency requirements, with some modifications, and believes they will promote accountability among BIAS providers.

On choice, the NPRM proposes three categories: (1) practices for which consent is implied, which would require no choice; (2) first-party and affiliate marketing of telecommunications services, which would require opt-out choice; and (3) other first-party uses and sharing with third parties, which would require opt-in choice.[29] As discussed further below, FTC staff agrees with some of these proposals but provides the FCC with some suggestions and

---

[25] *See, e.g.*, ScanScout, Inc., Docket No. C-4344 (Dec. 14, 2011) (decision and order) *available at* https://www.ftc.gov/enforcement/cases-proceedings/102-3185/scanscout-inc-matter (alleging that ad network told consumers they could opt out of tracking through browser settings, but continued to track consumers through Flash cookies).

[26] *See generally* Prepared Statement of the Fed. Trade Comm'n, *Data Breach on the Rise: Protecting Personal Information From Harm* at 9-11, Before the S. Comm. on Homeland Security & Governmental Affairs, 113th Cong. (Apr. 2, 2014), *available at* https://www ftc.gov/public-statements/2014/04/prepared-statement-federal-trade-commission-data-breach-rise-protecting-0; Commission Statement Marking the FTC's 50th Data Security Settlement (Jan. 31, 2014), *available at* https://www ftc.gov/news-events/blogs/business-blog/2014/01/50th-data-security-settlement-offers-golden-opportunity; FTC Report, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policy Makers at 11-14 (Mar. 2012), *available at* https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers ("Privacy Report").

[27] For example, if the FCC does not accept FTC staff's recommendations on choice, it may be necessary to revisit FTC staff's proposed definition of personally identifiable information.

[28] Privacy NPRM, Proposed Rule 47 C.F.R. § 64.7001.

[29] Privacy NPRM, Proposed Rule 47 C.F.R. § 64.7002.

alternatives on others to consider in light of the questions posed by the FCC regarding how choices should be provided.[30]

Finally, on security, FTC staff generally supports the approach articulated in the NPRM, subject to certain recommended changes. FTC staff also supports inclusion of a breach notification requirement for BIAS providers, again, subject to certain recommended changes.

In providing its comments, FTC staff is mindful that the FCC's proposed rules, if implemented, would impose a number of specific requirements on the provision of BIAS services that would not generally apply to other services that collect and use significant amounts of consumer data. This outcome is not optimal. The FTC has repeatedly called for Congress to pass additional laws to strengthen the privacy and security protections provided by all companies, however, including through baseline privacy, data security, and data breach notification laws applicable to all entities that collect consumer data.[31] FTC staff continues to believe that such generally applicable laws are needed to ensure appropriate protections for consumers' privacy and data security across the marketplace.

Staff also recognizes that the FCC will need to apply its own regulatory expertise in implementing these recommendations, in a manner consistent with its governing statutes and regulations. Accordingly, we have set forth general recommendations, with the intent that the FCC will draw on its own experience to apply them specifically to the provision of BIAS.

---

[30] Privacy NPRM, ¶ 116.

[31] *See, e.g.*, Privacy Report at 11-14; Internet of Things Report at 48-52; Prepared Statement of the Fed. Trade Comm'n, *Data Breach on the Rise: Protecting Personal Information From Harm* at 9-11, Before the S. Comm. on Homeland Security & Governmental Affairs, 113th Cong. (Apr. 2, 2014), *available at* https://www ftc.gov/public-statements/2014/04/prepared-statement-federal-trade-commission-data-breach-rise-protecting-0. Commissioner Ohlhausen has supported calls for Congressional action on data security and data breach notification, but believes the success of the FTC's current privacy regime mitigates the need for baseline privacy legislation.

## IV. DEFINING PERSONALLY IDENTIFIABLE INFORMATION

The definition of "personally identifiable information" ("PII") is central to the proposed rule's privacy and data security protections. The proposed rule would define PII as "any information that is linked or linkable to an individual."[32] BIAS providers that use and share PII would be subject to the FCC's proposed transparency, choice, and security requirements.

FTC staff agrees that the definition of PII should not be confined to information that is already linked to an individual. Advances in technology provide companies with the ability to identify consumers by combining disparate pieces of data.[33] Not only is it possible to link information historically considered non-PII to specific individuals or devices, but businesses have strong incentives to do so.[34] In recognition of this fact, the NPRM's inclusion of information that is "linkable" extends stronger privacy protections to consumers.

However, the proposal to include any data that is "linkable" could unnecessarily limit the use of data that does not pose a risk to consumers. While almost any piece of data *could* be linked to a consumer, it is appropriate to consider whether such a link is practical or likely in light of current technology. FTC staff thus recommends that the definition of PII only include information that is "reasonably" linkable to an individual.[35]

---

[32] Privacy NPRM, Proposed Rule 47 C.F.R. § 64.7000(j).

[33] Privacy Report at 20. *See also* Arvind Narayanan, Joanna Huey, & Edward W. Felten, *A Precautionary Approach to Big Data Privacy* at 5 (Mar. 19, 2015), *available at* http://randomwalker.info/publications/precautionary.pdf (recognizing that "[n]ew attributes continue to be linked with identities: search queries, social network data, genetic information (without DNA samples from the targeted people), and geolocation data all can permit re-identification. . . . The realm of potential identifiers will continue to expand, increasing the privacy risks of already released datasets.")

[34] Privacy Report at 20.

[35] *See, e.g.*, 45 C.F.R. § 160.103 (defining "individually identifiable health information" in the context of the Health Insurance Portability and Accountability Act as, *inter alia*, information "[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual").

Additionally, FTC staff recommends that the FCC consider tying "reasonable linkability" to both individuals and their devices.[36] For example, consumers' mobile handsets are extremely personal, almost always on, and almost always with the user.[37] As consumer devices become more personal and associated with individual users, the distinction between a device and its user continues to blur.[38] Accordingly, FTC staff recommends that the proposed Rule's definition of PII include information that is "linked or reasonably linkable to a consumer or a consumer's device." This definition would capture persistent identifiers such as cookies, static IP addresses, MAC addresses, and other device identifiers.

The FTC's Rule implementing the Children's Online Privacy Protection Act ("COPPA") includes persistent identifiers in the definition of personal information.[39] Furthermore, the FTC has brought enforcement actions to hold accountable companies that make, but then break, promises about how they use persistent identifiers.[40] For example, the FTC alleged that ad networks run by Chitika, Scanscout, and Google engaged in deceptive practices in connection with those companies' use of cookies for behavioral advertising.[41] Although most of these companies did not collect traditional categories of personal information, the FTC still held them

[36] Under FTC staff's proposed approach, personal information would not include information reasonably linkable to non-personal devices, such as an autonomous ride-sharing vehicle that can be summoned by any member of the public.
[37] Mobile Disclosures Report at 2.
[38] Mobile Disclosures Report at 2; Privacy Report at 2, 19.
[39] 16 C.F.R. § 312.2; *see also* 15 U.S.C. § 6501(8).
[40] *See, e.g.*, Epic Marketplace, Inc., Docket No. C-4389 (Mar. 13, 2013) (decision and order), *available at* https://www.ftc.gov/enforcement/cases-proceedings/112-3182/epic-marketplace-inc; Google Inc., Docket No. C-4336 (Oct. 13, 2011) (decision and order), *available at* https://www ftc.gov/enforcement/cases-proceedings/102-3136/google-inc-matter.
[41] ScanScout, Inc., Docket No. C-4344 (Dec. 14, 2011) (decision and order) *available at* https://www.ftc.gov/enforcement/cases-proceedings/102-3185/scanscout-inc-matter; Chitika, Inc., Docket No. C-4324 (June 17, 2011) (decision and order) *available at* https://www.ftc.gov/enforcement/cases-proceedings/1023087/chitika-inc-matter; Google Inc., Docket No. C-4336 (Nov. 20, 2012) (decision and order), *available at* https://www.ftc.gov/enforcement/cases-proceedings/102-3136/google-inc-matter.

to their promises about tracking technologies that used persistent identifiers associated with a device, rather than an individual.

Finally, the NPRM seeks comment on whether BIAS customers' names, postal addresses, and telephone numbers should be treated as PII.[42] The FTC has consistently treated name, address, and telephone number as fundamental components of PII in both its regulations and its orders.[43] Accordingly, FTC staff recommends that customer names, postal addresses, and telephone numbers be included in the definition of PII.

## V. TRANSPARENCY

The Proposed Rule would require a BIAS provider to "clearly and conspicuously notify its customers of its privacy policies," and sets forth proposed requirements for the content of the policies.[44] In addition to seeking comment on the proposed requirements, the FCC seeks comment on how companies should display the notices,[45] whether the notices should be standardized,[46] what language the notices should be offered in,[47] and how companies should address changes to the notices.[48]

FTC staff supports the proposed requirement to clearly and conspicuously disclose privacy policies. With respect to the content of the policies, FTC staff generally agrees with the categories of information that the FCC proposes be disclosed, which include the types of data

---

[42] Privacy NPRM, ¶¶ 45-46.
[43] *See, e.g.*, 16 C.F.R. § 312.2 (COPPA Rule); 16 C.F.R. § 313.3(n)(1)(ii) (financial privacy rules under Gramm-Leach-Bliley Act); Henry Schein Practice Solutions, Inc., Docket No. C-4575 (May 23, 2016) (decision and order), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3161/henry-schein-practice-solutions-inc-matter; Credit Karma, Inc., Docket No. C-4480 (Aug. 19, 2014) (decision and order), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3091/credit-karma-inc; Fandango LLC, Docket No. C-4481 (Aug. 19, 2014) (decision and order) *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3089/fandango-llc; HTC America, Inc., Docket No. C-4406 (July 2, 2013) (decision and order), *available at* https://www.ftc.gov/enforcement/cases-proceedings/122-3049/htc-america-inc-matter.
[44] Privacy NPRM, Proposed Rule 47 C.F.R. § 64.7001(a).
[45] Privacy NPRM, ¶¶ 66, 69.
[46] Privacy NPRM, ¶¶ 72-75.
[47] Privacy NPRM, ¶ 65.
[48] Privacy NPRM, ¶ 82.

collected in the course of providing BIAS, a description of the use and sharing of data, the categories of entities that will receive the data, and an explanation of how consumers can exercise choices. Disclosing this information provides an important accountability function. Privacy advocates, regulators, the press, consumers, and others will have access to information about how companies collect, use, and share data. The notices constitute public commitments regarding companies' data practices. In addition, in crafting their privacy policies, companies will engage in the exercise of reviewing their privacy practices and potentially discontinuing practices that are not warranted.

As to how the notices should be displayed, in addition to requiring that the notices be "clear and conspicuous," "comprehensible," and "legible," as the FCC has already proposed,[49] FTC staff recommends that the FCC take additional steps to encourage BIAS providers to make privacy notices clearer, shorter, and more standardized than they currently are.[50] Existing privacy notices are often difficult to comprehend. For example, in a study of mobile shopping app privacy policies, FTC staff found that nearly all of the app privacy policies it reviewed "contained broad and vague statements" that made it difficult for consumers to assess how their data was actually used.[51] FTC staff found that these types of vague disclosures preserve broad

[49] Privacy NPRM, Proposed Rule 47 C.F.R. § 64.7001.
[50] Privacy Report at 60; FTC Staff Report, *What's the Deal? An FTC Study on Mobile Shopping Apps* at 24-25 (Aug. 2014), *available* at https://www ftc.gov/reports/whats-deal-federal-trade-commission-study-mobile-shopping-apps-august-2014 ("Mobile Shopping App Report"); *see also* Privacy NPRM, ¶¶ 72-73.
[51] Mobile Shopping App Report at 21.

rights for companies but fail to achieve the central purpose of a privacy notice: to make clear how data is collected, used, and shared.[52]

To achieve the goals of clarity, brevity, and comparability, the FCC should consider developing a standardized or "model" notice[53] based on consumer testing, similar to that conducted by the FTC and seven other agencies when they undertook to develop a model financial privacy notice.[54] Standardization of privacy notices can better enable consumers to comprehend and compare privacy practices. Standardization also encourages companies to compete on privacy.[55] And standardization, with shorter notices, will be particularly essential as consumers increasingly rely on mobile devices with small screens and little opportunity to read disclosures.[56]

---

[52] Mobile Shopping App Report at 25. *See also* Data Broker Report at 42 ("[D]ata brokers provide notice on their website, typically within a lengthy privacy policy, and an explanation of how to access the information; however, these notices may be hard to understand."); Kirsten Martin, *Privacy Notices as Tabula Rasa: An Empirical Investigation into How Complying with a Privacy Notice Is Related to Meeting Privacy Expectations Online*, Journal of Public Policy & Marketing, Vol. 34, No. 2 (Fall 2015), *available at* http://journals.ama.org/doi/full/10.1509/jppm.14.139 (finding that consumers incorrectly interpret privacy policies, believing them to protect more information than they do).

[53] The FCC took this approach with respect to broadband pricing labels. FCC, Press Release, FCC Unveils Consumer Broadband Labels to Provide Greater Transparency to Consumers (Apr. 4, 2016), *available at* https://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db0404/DOC-338708A1.pdf.

[54] *See, e.g.*, FTC, Financial Privacy Rule: Interagency Notice Research Project, *available at* https://www.ftc.gov/tips-advice/business-center/guidance/financial-privacy-rule-interagency-notice-research-project (describing results of GLB short notice interagency effort between FTC, FRB, OCC, FDIC, SEC, NCUA, OTS, and CFTC). As described in a 2014 report, the FTC's consumer testing showed certain important attributes for financial privacy notices: (1) simplicity; (2) good design techniques; (3) neutrality in language and presentation; (4) context; and (5) standardization. Mobile Disclosures Report at 8. Consumer testing may reveal differences in desirable attributes for policies concerning the provision of BIAS; staff is not advocating a one-size-fits-all approach. Slightly modified standard formats may work for different industries.

[55] Privacy Report at 61. This may already be happening. The FTC Staff's Mobile Disclosures Report cited a nationwide survey indicating that 57% of all app users have either uninstalled an app over concerns about having to share their personal information, or declined to install an app in the first place for similar reasons. Mobile Disclosures Report at 3.

[56] *See* Mobile Disclosures Report at 25-28; Mobile Shopping App Report at 24-25. Consumer testing may reveal that a mobile disclosure should look different from a web-based disclosure. If so, the FCC could consider two model notices – one for the web and one for mobile.

In addition, to provide companies with greater certainty, and an incentive to use the model notice, FTC staff recommends that the FCC provide a safe harbor, making clear that use of the model notice constitutes compliance with the rule's notice requirements.

The Proposed Rule would further require that BIAS providers translate all portions of a privacy notice into another language if any portion of a notice is translated into that language.[57] FTC staff supports a slightly modified approach – namely, that if a subscriber transacts business with the BIAS provider in a language other than English, the BIAS provider should translate the privacy notice into that language. This approach follows the FTC's Business Opportunity Rule and policy statement on foreign language advertising, both of which require that if a company advertises or offers a product for sale in a language other than English, the company should also translate any material disclosures into that language.[58]

Finally, the NPRM suggests requiring BIAS providers to give consumers advance notice of material changes to privacy policies, but does not require the BIAS providers to obtain affirmative express consent before making changes that apply to previously collected consumer information.[59] The FTC's long-standing position is that affirmative express consent should be required before a company makes such "material retroactive changes" to its privacy policy.[60] The FTC first articulated this principle in its 2004 case against Gateway Learning, where it alleged that after collecting consumers' information under a policy promising that the company would not share consumers' information with third parties, the company changed its privacy policy to allow sharing without notifying consumers or getting their consent. The FTC alleged

[57] Privacy NPRM, Proposed Rule 47 C.F.R. § 64.7001(a)(7); *see also* Privacy NPRM, ¶ 65.
[58] *See* Business Opportunity Rule, 16 C.F.R. § 437.3(a); Requirements concerning clear and conspicuous disclosures in foreign language advertising and sales materials, 16 C.F.R. § 14.9.
[59] Privacy NPRM Proposed Rule 47 C.F.R. § 64.7001(c).
[60] The FTC's position applies to retroactive changes. It will likely be sufficient to provide robust notice and an opportunity to opt out for prospective changes in most instances. Privacy Report at 58.

that this was an unfair practice.[61] Similarly, in its case against Facebook, the FTC alleged that Facebook made certain user profile information publicly available that was previously subject to users' privacy settings, and thus materially changed its promises to consumers without obtaining their consent.[62]

Requiring consumers to provide affirmative express consent before making material retroactive changes is essential to privacy protection. Absent such a requirement, companies could offer robust privacy notices to attract consumers, and collect their data, and then, at a later date, ratchet down protections on that data.[63]

## VI. CHOICE

The NPRM and the proposed rule propose three categories of choice for information use and sharing practices: (1) those for which consent is implied; (2) opt-out for first party and affiliate marketing of communications-related services; and (3) opt-in for other first-party uses and sharing with third parties.[64] This comment discusses all three categories.

### A. Practices For Which Consent is Implied

FTC staff generally agrees with the NPRM's designation of certain practices for which consent is implied and explicit consent is not required. As the FTC has stated, consent may be inferred for collection, sharing, and use that is within consumer expectations – *i.e.*, consistent

---

[61] Gateway Learning Corp., Docket No. C-4120 (Sept. 17, 2004) (decision and order) *available at* https://www.ftc.gov/enforcement/cases-proceedings/042-3047/gateway-learning-corp-matter.

[62] Facebook, Inc., Docket No. C-4365 (Aug. 10, 2012) (decision and order) *available at* https://www.ftc.gov/enforcement/cases-proceedings/092-3184/facebook-inc.

[63] Another fundamental component of transparency is the ability to access information. The NPRM asks whether consumers should have the right to access the data BIAS providers have gathered and inferred about them, and whether consumers should have the right to correct any such data. Privacy NPRM, ¶¶ 187-91. FTC staff recommends that if a BIAS provider uses a consumer's data for marketing purposes, the consumer should be able to access, at a minimum, the categories of information that the provider holds about them, along with the ability to suppress the use of such categories for marketing. However, if the BIAS provider uses a consumer's data to determine eligibility for a new product or benefit, then the consumer should have access to the actual data used to make the decision, along with the ability to correct it. Privacy Report at 64-68. The required level of access and correction should also be tied to the importance of the benefit or transaction in question, and should not undermine the development of accurate risk mitigation tools. Data Broker Report at 54.

[64] Privacy NPRM, Proposed Rule 47 C.F.R. § 64.7002.

with the context of the transaction or the consumer's existing relationship with the business.[65] Consistent with this approach, the proposed rule provides several categories of information for which no notice and consent is necessary, including that used for billing and other functions necessary to complete provision of BIAS providers' services,[66] as well as aggregate information that does not identify individual consumers.[67] FTC staff suggests that the FCC clarify that, when consent is implied, BIAS providers may use consumers' data solely for the provision of BIAS services and for no other purposes. This may require contractual protections requiring data recipients to use the data for the purposes enumerated in the Rule and for no other purpose. In addition, FTC staff provides comments, below, on two specific practices in this category: sharing information, including geolocation, with family members in emergency situations; and sharing information related to unwanted, abusive, or illegal calls.

### 1. Emergency Situations

The NPRM proposes that, in emergency situations, BIAS providers be permitted to share consumers' information with family members.[68] Although access to family would be helpful in the vast majority of cases, consumers could be harmed if their information were exposed to abusive family members. The FTC has experience with this issue. In its case against data broker Accusearch, company representatives purported to seek access to their own accounts when, in

[65] Privacy Report at 27, 36-40; Internet of Things Report at 40-41.
[66] Privacy NPRM, Proposed Rule 47 C.F.R. § 64.7002(a), ¶¶ 97-98.
[67] The Proposed Rule allows the use and disclosure of aggregate customer information if the BIAS provider (1) determines that the information is not reasonably linkable to a specific individual; (2) publicly commits not to re-identify such information; (3) contractually restricts third parties from re-identifying the information; and (4) exercises reasonable monitoring over those contractual provisions. Privacy NPRM, Proposed Rule 47 C.F.R. § 64.7002(g). This is consistent with the FTC's past recommendations that appropriately de-identified data may be shared without consumer consent. *See, e.g.*, Privacy Report at 20-22 (setting out guidelines for use of de-identified data); *see also* Internet of Things Report at 37-38 (suggesting that data may be stored in de-identified form to protect it).
[68] Privacy NPRM, Proposed Rule 47 C.F.R. § 64.7002(a)(5); Privacy NPRM, ¶ 98.

reality, they were trying to gain access to other people's confidential telephone records.[69] The court found that this activity exposed consumers to "severe harm . . . from stalkers and abusers who procured the consumers' phone records," and constituted "a clear and unwarranted risk to those consumers' health and safety."[70] Likewise, the FTC's complaint against Google for its launch of the Buzz social network alleged that the company used consumers' email contacts to automatically set up consumers with "followers," who were given access to some of the consumers' PII.[71] In some cases, the followers were persons against whom consumers had obtained restraining orders and abusive ex-husbands.[72]

To protect against this danger, FTC staff recommends that the FCC consider safeguards, such as asking consumers to designate in advance family members authorized to access their personal information. Alternatively, the FCC could follow the model set forth in the FTC's Health Breach Notification Rule, which requires that if a consumer wants their next of kin notified of a breach of the consumer's personal health record, the individual must provide contact information and an authorization.[73]

### 2. Unwanted, Abusive, and Illegal Calls

The NPRM proposes to allow BIAS providers and telecommunications carriers[74] to share calling party phone numbers, including "spoofed" numbers, associated with abusive, fraudulent,

---

[69] *FTC v. Accusearch, Inc.*, 570 F.3d 1187, 1191-92 (10th Cir. 2009).
[70] *FTC v. Accusearch, Inc.*, 2007 WL 4356786 at *8 (D. Wyo. Sept. 28, 2007), *aff'd* 570 F.3d 1187 (10th Cir. 2009).
[71] *Google, Inc.*, Docket No. C-4336 at 2-5 (Oct. 13, 2011) (decision and order), *available at* https://www.ftc.gov/enforcement/cases-proceedings/102-3136/google-inc-matter.
[72] *Id.*
[73] 16 C.F.R. § 318.5(a)(1).
[74] Privacy NPRM, Proposed Rule 47 C.F.R. § 64.7002(a)(3) applies to BIAS providers. However, the FCC also proposes to interpret Section 222(d)(2) "to allow *telecommunications carriers* to use or disclose" information relating to abusive, fraudulent, or unlawful robocalls. Privacy NPRM, ¶ 100 (emphasis added). Although most of this comment focuses on the application of the FCC's proposed rules to BIAS providers, FTC staff has unique experience in the telemarketing area; accordingly, in this section, the FTC staff makes recommendations with respect to both BIAS providers and telecommunications carriers.

or unlawful robocalls.[75] Consumer demand for call-blocking or call-filtering technologies is high,[76] and FTC staff supports the FCC's proposal, which will improve the effectiveness of such solutions.

However, FTC staff recommends that the FCC expand this proposal in two ways. First, it should allow the sharing of calling party phone numbers not only for robocalls, but for all calls that a consumer identifies as being abusive, fraudulent, or unlawful. FTC complaint data indicates that consumers are harassed by a deluge of unwanted calls from live telemarketers in addition to robocalls. From October 2014 to September 2015, the FTC received over 3.5 million Do-Not-Call complaints, of which approximately 40% (over 1.4 million) did not involve a robocall.[77] Moreover, as of September 2015, the National Do Not Call Registry included 222 million phone numbers, indicating these consumers' preference not to receive unsolicited telemarketing sales calls from live operators.[78]

Second, FTC staff recommends that the FCC permit BIAS providers and telecommunications carriers to share not only calling party phone numbers, but also any other information these entities need to locate or identify a particular abusive, fraudulent, or unlawful robocall or live call that traversed their networks. Such information may include the date and time of the call, the carrier that passed the call on to its network, the carrier the call was passed

[75] Privacy NPRM, ¶ 100.
[76] *See* FTC Staff, Comments Before the Federal Communications Commission on Public Notice DA 14-1700 Regarding Call Blocking, CG Docket No. 02-278; WC Docket No. 07-135 (Jan. 23, 2015), *available at* https://www.ftc.gov/policy/policy-actions/advocacy-filings/2015/01/ftc-staff-comment-federal-communications-commission.
[77] *See* FTC, *National Do Not Call Registry Data Book FY 2015* at 5 (Nov. 2015), *available at* https://www.ftc.gov/reports/national-do-not-call-registry-data-book-fiscal-year-2015.
[78] *See id.* at 4.

on to, SS7 or SIP signaling information (*e.g.*, point codes), and IP information (*e.g.*, IP address, domain names, and registrar information).[79]

New technologies allow callers to spoof caller ID information, and thus avoid detection, hide the caller's identity, and mask the true origin of the call. As a result, BIAS providers and telecommunications carriers will likely know little about the origin of the call.[80] Allowing BIAS providers and telecommunications carriers to share information that enables tracing a call to its originating point would significantly enhance efforts to combat abusive, fraudulent, or unlawful calls, and improve call-blocking or call-filtering technologies to provide greater protections to consumers.

### B. Practices That Require Choice

As noted above, the FCC proposes that BIAS providers provide opt-out consent for first-party and affiliate marketing of communications-related services and opt-in for other first-party uses and sharing with third parties. FTC staff offers its views on this approach in response to the FCC's solicitation for comment on categories of information for which choice should be required.

#### 1. Practices that Require Opt-In

The FTC's general approach to consumer choice has focused on whether the collection and use of information is consistent with the context of a consumer's interaction with a company and the consumer's reasonable expectations.[81] For practices that are inconsistent with such

[79] Because consumers report abusive, fraudulent, or unlawful calls with the expectation that the entity receiving their complaints – law enforcement or their carrier – will take necessary action, BIAS providers and telecommunications carriers should also be allowed to use and share the call recipient's phone number, as long as they provide the consumer an opportunity to opt out before the consumer's number is shared.

[80] *See* Prepared Statement of the Federal Trade Commission, *Combatting Illegal Robocalls: Initiatives to End the Epidemic* at 11-12, Before the S. Special Comm. on Aging, 114th Cong. (June 10, 2015), *available at* https://www.ftc.gov/public-statements/2015/06/prepared-statement-federal-trade-commission-combatting-illegal-robocalls.

[81] *See, e.g.*, Privacy Report at 27, 36-40; Internet of Things Report at 40-41.

interactions and expectations, the FTC has advocated that companies provide meaningful choices to consumers, with the level of choice being tied to consumer expectations. Under this approach, the FTC supports the use of opt-in for sensitive information that could be collected by BIAS providers, including: (1) content of communications and (2) Social Security numbers or health, financial, children's, or precise geolocation data.

The FTC supports using opt-in for the *content* of consumer communications regardless of whether the company is a first party, affiliate, or third party.[82] The term "content" includes consumer communications such as contents of emails; communications on social media; search terms; web site comments; items in shopping carts; inputs on web-based forms; and consumers' documents, photos, videos, books read, movies watched – all of which applies whether a consumer uses a traditional computer or an Internet-connected device.[83] Content data can be highly personalized and granular, allowing analyses that would not be possible with less rich data sets.[84] It also can be used to infer additional information about consumers, including sensitive information, and to make decisions about consumers that may harm them, especially if the data or the inferences are inaccurate.[85]

As the FTC discussed in its 2012 Privacy Report, BIAS providers have the opportunity to collect a wide range of content, as their customers interact with many different companies across the entire Internet offering diverse products and services.[86] They also can use deep packet inspection ("DPI"), which refers to BIAS providers' ability to analyze the data packets that

[82] *See*, *e.g.*, Privacy Report, at 55-56.
[83] The term content should not include a persistent identifier only.
[84] Internet of Things Report at 15; *see also* Data Broker Report at 46-47.
[85] Data Broker Report at 47-48; Internet of Things Report at 15-17.
[86] Other large platforms may also comprehensively track consumers, such as through the use of social plugins. *See* Privacy Report at 40-41; FTC Workshop, "The Big Picture: Comprehensive Data Collection (Dec. 6, 2012), https://www.ftc.gov/news-events/events-calendar/2012/12/big-picture-comprehensive-online-data-collection.

traverse their networks when consumers use their services.[87] As stated in the Commission's 2012 report, "the Commission has strong concerns about the use of DPI for purposes inconsistent with an ISP's interaction with a customer, without express affirmative consent or more robust protection."[88] Under the FCC's proposal, BIAS providers could use content of communications for internal and affiliate marketing without obtaining consumers' opt-in consent first. This would mean, for example, that a provider could use information from a consumer's online search or shopping history to determine that the consumer can afford a more expensive product, and upsell the consumer accordingly, subject only to opt-out choice. The provider also could share that information with its affiliates, again subject only to an opt-out. FTC staff believes that consumers should have opt-in choice for such uses of data.

Although paragraph 49 of the NPRM notes that the FCC does not "think that providers should ever use or share the content of communications that they carry on their network without having sought and received express, affirmative consent for the use and sharing of content," the text of the Proposed Rule does not appear to reflect this approach. FTC staff proposes that the Proposed Rule be revised to clearly require choice for the contents of consumer communications.

The FTC also has supported the use of opt-in for the collection, use, and sharing information of sensitive data (*e.g.*, Social Security numbers and children's, financial, health, and geolocation data[89]) because the more sensitive the data, the more consumers expect it to be protected and the less they expect it to be used and shared without their consent.[90] For example,

---

[87] Privacy Report at 40 n.189.
[88] Privacy Report at 56.
[89] *Id.* at 40 n.189, 47-48, 58-60.
[90] *See* Rafi Goldberg, *Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities*, NTIA (May 13, 2016), *available at* https://www.ntia.doc.gov/print/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities (finding that consumers express more concern about the privacy and security of data that can be used for identity theft, and show more reluctance to engage in financial transactions than posting on social networks).

if the FCC were to adopt this approach, a BIAS provider would have to obtain opt-in consent to use consumer data on sensitive health sites or from sensitive devices such as blood glucose or blood pressure monitors, regardless of whether such data were used for first-party marketing or shared with third parties. Notably, if the FCC were to adopt FTC staff's recommendation for opt-in consent before use of the content of consumer communications, BIAS providers would not be permitted to inspect the contents of such communications to determine whether they are sensitive.[91]

In contrast to the FTC's approach, the NPRM proposes to distinguish between first-party and affiliate marketing of communications-related services on the one hand, and other first-party uses and sharing with third parties on the other. FTC staff believes that there may be some advantages to this approach. It generally tracks the precedent laid out years ago in the FCC's existing CPNI Rule, which applies to some of the same entities covered under the Proposed Rule.[92] It creates a bright line for industry to follow, which may facilitate compliance and law enforcement. And it protects consumers from unknown uses by third parties with which they have no relationship.[93] However, this approach does not reflect the different expectations and concerns that consumers have for sensitive and non-sensitive data. As a result, it could hamper beneficial uses of data that consumers may prefer, while failing to protect against practices that are more likely to be unwanted and potentially harmful. For example, consumers may prefer to

[91] The prohibitions on use of sensitive information for marketing are consistent with existing approaches implemented by ad networks and mobile platforms. *See, e.g.*, 2015 Update to the NAI Code of Conduct, Network Advertising Initiative at 6, 14-15 (2015), *available at* https://www.networkadvertising.org/sites/default/files/NAI_Code15encr.pdf (requiring *inter alia*, opt-in consent when targeted advertising is based on an inferred interest in sensitive health information); Mobile Disclosures Report at 17-18 (describing how Apple and Google have implemented opt-in requirements for collection of geolocation in their iOS and Android products).

[92] The proposed rule, however, would expand the volume and variety of data covered.

[93] As noted below, consumers may not have any relationship or knowledge of affiliates either, which should be treated as third parties in certain circumstances.

hear about new innovative products offered by their BIAS providers, but may expect protection against having their sensitive information used for this or any other purpose. Therefore, FTC staff recommends that the FCC consider the FTC's longstanding approach, which calls for the level of choice to be tied to the sensitivity of data and the highly personalized nature of consumers' communications in determining the best way to protect consumers.[94]

Regardless of whether the choice is opt-in or opt-out, FTC staff continues to believe that, when consumers have few options for broadband service, the BIAS provider should not condition the provision of broadband on the customer's agreeing, for example, to allow the provider to track all of the customer's online activity for marketing purposes in a take-it-or-leave-it offer.[95] Further, as discussed below, the manner of choice – including timing and format – is of critical importance in ensuring that a consumer's choice is meaningful and informed.

### 2. Treatment of Affiliates

The Proposed Rule would allow sharing with affiliates for purposes of marketing communications-related services to consumers, subject to the opportunity to opt out.[96] The Proposed Rule defines "affiliate" with reference to common ownership or control but seeks comment on this definition.[97] The FTC has recommended that affiliates be treated as third parties, unless the affiliate relationship is clear to consumers.[98] Otherwise, from the consumer's perspective, an affiliate could be akin to a third party, depending on the type of companies at

[94] This approach is also consistent with existing international frameworks, such as the OECD Privacy Guidelines, which distinguish between sensitive and non-sensitive information. *See., e.g.*, OECD Privacy Framework at 16 ¶¶ 15(a)(ii), 18 (2013), *available at* http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.
[95] Privacy Report at 51-52. Where there are sufficient alternatives, however, the FTC noted in its 2012 Privacy Report that "take-it-or-leave-it choice can be acceptable, provided that the terms of the exchange are transparent and fairly disclosed . . . ." *Id.*
[96] Privacy NPRM, Proposed Rule 47 U.S.C. § 64.7002(e)(2); *see also* Privacy NPRM, ¶ 114.
[97] Privacy NPRM, Proposed Rule 47 C.F.R. § 64.2003(c); Privacy NPRM, ¶ 12.
[98] Privacy Report at 42.

issue and their data practices. Common branding is one way of making the affiliate relationship clear to consumers.[99] While consumers may expect "Cable Corporation" and "Cable Inc." to share information for marketing communications-related services, they are unlikely to expect Cable's parent-company, "Television, Inc.," to share such information. Therefore, if the FCC retains its current distinction among first parties, affiliates, and third parties, FTC staff believes that sharing of information among non-commonly branded affiliates is more akin to third-party sharing, and should be treated in the same manner as third-party sharing.

### 3. Manner of Presenting Choices

The manner of presenting choices is also very important. For example, an opt-in choice could be buried in a lengthy Terms of Use, while opt-out could be presented clearly and prominently. The Proposed Rule would require that BIAS providers offer consumers choices at the time the providers intend to use or disclose the consumers' information.[100] It is unclear whether the FCC intends for BIAS providers to offer such choices at the time of sign-up, at a point when the consumer first goes online, or at a point when the BIAS provider shares a consumer's data with an affiliate or third party.

The FTC has long advocated that companies offer choices to consumers at a "just-in-time" point. That is, companies should offer the choice at a time and in a context in which the consumer is making a decision about his or her data.[101] By informing consumers at an appropriate moment in time, a disclosure is likely to be of greater relevance to them.[102]

For BIAS providers, FTC staff believes that the most relevant time is when the consumer signs up for service, because this is the time when the consumer will likely be considering

[99] *Id.*
[100] Privacy NPRM, Proposed Rule 47 C.F.R. § 64.7002(c); *see also* Privacy NPRM, ¶ 121.
[101] Privacy Report at 48; Mobile Disclosures Report at 15-16.
[102] Mobile Disclosures Report at 11.

material terms. Accordingly, as an alternative to the FCC's proposed approach, FTC staff recommends that the FCC require BIAS providers to present consumers with a just-in-time choice upon sign up.

As the FCC recognizes, the choice should be presented in a clear and prominent manner; should not be buried in lengthy "terms and conditions"; and should not be accompanied by long, incomprehensible text. FTC staff recommends that the FCC require the BIAS provider to provide a short and clear explanation of the choice, accompanied by equally prominent "yes" and "no" buttons or checkboxes, on a separate page, outside of an end user licensing agreement ("EULA") or privacy policy or similar document. This approach is consistent with a number of FTC privacy orders, which require certain privacy disclosures and choices to be made clearly, prominently, and separately from any privacy notice. The orders generally state that companies must make the relevant privacy disclosures about information collection and use "[c]learly and prominently, immediately prior to the initial collection of or transmission of [] information, and on a separate screen from any final 'end user license agreement,' 'privacy policy,' 'terms of use' page, or similar document."[103] It is also consistent with a requirement contained in the Fair Credit Reporting Act ("FCRA") regarding employment background checks. The FCRA requires employers seeking background checks on consumers to provide a clear and conspicuous written disclosure to the consumer – *in a document that consists solely of the disclosure* – that the employer will obtain a consumer report.[104]

---

[103] *See, e.g.*, Goldenshores Techs., LLC, Docket No. C-4446 (Mar. 31, 2014) (decision and order), available at https://www.ftc.gov/enforcement/cases-proceedings/132-3087/goldenshores-technologies-llc-erik-m-geidl-matter; DesignerWare, LLC, Docket No. C-4390 (Apr. 11, 2013) (decision and order), *available at* https://www.ftc.gov/enforcement/cases-proceedings/112-3151/designerware-llc-matter; Facebook, Inc., Docket No. C-4365 (July 27, 2012) (decision and order), *available at* https://www ftc.gov/enforcement/cases-proceedings/092-3184/facebook-inc.

[104] 15 U.S.C. § 1681b(b)(2)(A)(i).

Using this approach, BIAS providers would have the flexibility to provide the just-in-time choice in a variety of innovative ways, using a variety of user interfaces, including through set-up wizards. BIAS providers should apply the same type of creativity they rely on to develop effective marketing campaigns and user interfaces to consumer choice mechanisms.[105] They should also examine the effectiveness of choice mechanisms periodically to determine whether they are sufficiently prominent, effective, and easy to use.[106] Consumer testing will be important in this regard.

Finally, the FCC should require that the choices offered be easy to exercise. For example, the CAN-SPAM Rule, issued and enforced by the FTC, prohibits a company from requiring a consumer to do anything more than send a reply email or visit a single webpage to opt out of commercial emails.[107] This requirement has in turn encouraged an industry standard of including a single-click "unsubscribe" button in commercial emails as a simple way for consumers to exercise their rights under CAN-SPAM. At the other extreme, requiring a consumer to send a letter or create an account is not a reasonable opportunity for the consumer to make a choice. [108]

FTC staff also recommends that, as a complement to the just-in-time choice mechanism described above, the FCC require BIAS providers to include privacy settings menus on their websites and apps so that consumers can revisit the choices they made upon sign-up. The FTC staff's Mobile Disclosures Report, for instance, noted that a "privacy dashboard" provides an

---

[105] Privacy Report at 50; *see also* Internet of Things Report at 41-42 (discussing various options for providing effective notice and choice); Mobile Disclosures Report at 17-18 (discussing development of icons and importance of consumer testing).
[106] Privacy Report at 50; Mobile Disclosures Report at 17-18.
[107] 16 C.F.R. § 316.5.
[108] FTC, Health Breach Notification Rule; Final Rule, 16 C.F.R. Part 318, 74 Fed. Reg. 42962, 42972 (Aug. 25, 2009), *available at* https://www.ftc.gov/system/files/documents/federal_register_notices/2009/08/healthbreachnotificationrulefinal.pdf ("Health Breach Notification Rule").

easy way for consumers to determine which apps have access to which data and to revisit the choices they initially made about the apps.[109]

## VII. SECURITY

### A. Security Program Requirements

The FTC has taken a technology-neutral, process-based approach to security for two decades. This approach describes the steps a business should take to develop reasonable data security practices – with an emphasis on risk management – instead of enumerating particular technological measures. For example, in its Safeguards Rule implementing the data security requirements of the Gramm-Leach-Bliley Act,[110] and in dozens of data security consent decrees, the FTC has required companies to have a written comprehensive information security program that includes a designated official to run the program, an annual risk assessment, appropriate safeguards to address risks, service provider supervision, and periodic re-assessment of the program.[111] This approach protects consumers from lax data security practices, while also giving businesses the flexibility to tailor their programs to their particular circumstances.

The NPRM appears to require a similar approach, stating that security practices should be "calibrated to the nature and scope of the BIAS provider's activities, the sensitivity of the underlying data, and technical feasibility."[112] However, the proposed rule text would impose strict liability on companies for "ensuring" security.[113] FTC staff suggests modifying the language to require BIAS providers to "ensure the *reasonable* security, confidentiality, and

---

[109] Mobile Disclosures Report at 16; *see also* Internet of Things Report at 42 (recommending dashboard or command center where consumers can set privacy choices).
[110] 15 U.S.C. § 6801(b); 16 C.F.R. §§ 314.3-314.4.
[111] *See generally* FTC, Privacy and Security Cases, https://www ftc.gov/datasecurity.
[112] Privacy NPRM, ¶ 151.
[113] *Compare* Privacy NPRM, Proposed Rule 47 C.F.R. § 64.7005(a) *with* 64.7005(b) ("A BIAS provider may employ any security measures that will allow the provider to *reasonably* implement the requirements set forth . . . .") (emphasis added).

integrity of all customer PI . . . ." Assuming this change, the FTC staff generally supports the approach to data security set forth in the NPRM.

This comment makes three additional suggestions to enhance the protections provided by the proposed rules. First, the FCC should include a requirement that BIAS providers develop *written* comprehensive information security programs. It is essential to compliance and accountability that any information security program be written, in order to permit internal and external auditors to measure the effectiveness of the program and to provide for continuity as staff members leave and join the team. For this reason, all of the FTC's data security settlements,[114] as well as the Safeguards Rule,[115] require written programs.

Second, the NPRM seeks comment on whether and how companies should be obligated to dispose of consumer data.[116] The FTC, pursuant to the Fair and Accurate Credit Transactions Act of 2003 (FACTA) amendments to the FCRA, promulgated the Disposal Rule to address the process for destruction of consumer report-related information. When a company disposes of covered information, the Disposal Rule requires it to "dispose of [consumer] information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal."[117] The Rule identifies examples of compliant disposal methods, including the "burning, pulverizing, or shredding of papers" and "destruction or erasure of electronic media."[118] Alternatively, businesses that are subject to the rule can contract with a

[114] *See, e.g.*, GMR Transcription Servs. Inc., Docket No. C-4482 (Aug. 14, 2014) (decision and order) ("Such program, the content and implementation of which must be fully documented in writing . . . ."), *available at* https://www.ftc.gov/enforcement/cases-proceedings/122-3095/gmr-transcription-services-inc-matter.
[115] 16 C.F.R. § 314.3(a) (entity must "develop, implement, and maintain a comprehensive information security program that is written").
[116] Privacy NPRM, ¶¶ 212-14.
[117] 16 C.F.R. § 682.3(a).
[118] 16 C.F.R. § 682.3(b)(1)-(2).

third party to conduct disposal, provided that they properly supervise the third party.[119] FTC staff suggests that the FCC include disposal requirements that are similar to those contained in the FTC's Disposal Rule.[120]

Third, the NPRM asks whether the FCC should establish data security safe harbors.[121] FTC staff supports the development of data security safe harbors, but only if they include strong and concrete requirements backed by vigorous enforcement. Staff's recommendation is informed by the FTC's experience with safe harbors. For example, in COPPA, Congress included a provision enabling industry groups or others to submit for FTC approval self-regulatory programs that implement the protections of the FTC's COPPA rule.[122] These programs must include: (1) a requirement that participants implement substantially similar or more robust requirements than those contained in the Rule; (2) an effective, mandatory mechanism for the independent assessment of participants' compliance with the requirements; and (3) disciplinary actions for noncompliance.[123] The safe harbor programs have benefited businesses and consumers by providing clarity and certainty, creating an oversight regime to improve compliance, and preserving FTC resources to pursue the more egregious violations.[124]

Similarly, in its settlement with Wyndham Hotels and Resorts, the FTC's Order requires Wyndham to maintain a comprehensive information security program for payment card data. The Order allows Wyndham to obtain a safe harbor from enforcement if it passes an annual assessment conducted under the Payment Card Industry Data Security Standard ("PCI-DSS"),

---

[119] 16 C.F.R. § 682.3(b)(3).
[120] The Disposal Rule does not mandate when information should be disposed of, but how. FTC staff suggests a similar approach here.
[121] Privacy NPRM, ¶ 160.
[122] 15 U.S.C. § 6503.
[123] 16 C.F.R. § 312.11(b).
[124] *See* FTC, Press Release, *Revised Children's Online Privacy Protection Rule Goes Into Effect Today* (July 1, 2013), *available at* https://www ftc.gov/news-events/press-releases/2013/07/revised-childrens-online-privacy-protection-rule-goes-effect.

which largely mirrors the requirements contained in the order.[125] But, to ensure that the safe harbor is robustly implemented, the Order provides important additional safeguards. For example, if the FTC can show deception in the PCI-DSS assessment process, or a significant change in Wyndham's security program since its last assessment, Wyndham loses the safe harbor.

Appropriately crafted and robust safe harbors can provide additional regulatory certainty for businesses and improve consumer protections by encouraging companies and self-regulatory organizations to adhere to high standards. FTC staff believes any security safe harbors should require strong security measures that meet or exceed those reflected in the final rule, contain independent auditing and enforcement mechanisms, and ensure that any standards evolve with changing technology and business models.

### B. Breach Notification

FTC staff supports the FCC's inclusion of a breach notification provision in the proposed rule. The FTC has long supported federal breach notification legislation for all entities that collect and store consumer data.[126] Also, in 2009, the FTC promulgated its Health Breach Notification Rule, which applies to vendors of personal health records and related entities.[127] FTC staff applies this experience in providing comments on several aspects of the NPRM.

First, as to the appropriate breach trigger, the NPRM proposes that consumers be notified of a breach, which is defined as "any instance in which a person, without authorization or

---

[125] *FTC v. Wyndham Worldwide Corp.*, Case No. 2:13-cv-01887 (Stipulated Order for Injunction) (D.N.J. Dec. 11, 2015), *available at* https://www ftc.gov/enforcement/cases-proceedings/1023142-x120032/wyndham-worldwide-corporation.

[126] *See, e.g.*, Prepared Statement of the Fed. Trade Comm'n, *Data Breach on the Rise: Protecting Personal Information From Harm* at 9-11, Before the S. Comm. on Homeland Security & Governmental Affairs, 113th Cong. (Apr. 2, 2014), *available at* https://www ftc.gov/public-statements/2014/04/prepared-statement-federal-trade-commission-data-breach-rise-protecting-0.

[127] 16 C.F.R. Part 318.

exceeding authorization, has gained access to, used, or disclosed customer proprietary information."[128] This broad proposal raises two concerns. The first concern is that because the definition includes unauthorized access to *any* customer proprietary information, companies that only collect data such as device identifiers or information held in cookies may be required to collect *other* consumer information such as email addresses in order to provide consumers with breach notification.[129] For example, this could effectively prohibit BIAS providers,[130] from maintaining only anonymous browsing information, and instead, require them to link browsing with account information, so that they could notify customers of a breach involving any kind of persistent identifier.

A second concern is overnotification. If, for example, a company's employee were to inadvertently access a document, but not read it, should a consumer receive a notice? As the FTC noted in the Statement of Basis and Purpose to its Health Breach Notification Rule, when consumers receive "a barrage of notices" they could "become numb to such notices, so that they may fail to spot or mitigate the risks being communicated to them."[131] Indeed, a 2014 study by the Ponemon Institute found that almost half of the consumers surveyed had been victims of a data breach, and of those, 32% did nothing after receiving a notification, and only 18% took the

[128] Privacy NPRM, Proposed Rule 47 U.S.C. §§ 64.2003(d), 64.7000(b); *see also* § 64.7006.
[129] *See, e.g.*, Health Breach Notification Rule, 74 Fed. Reg. at 42972 (noting that some notice requirements "would result in entities' collecting additional personal information they otherwise would not collect, and that consumers may not want to provide").
[130] The NPRM proposes two breach notification rules, one for BIAS providers (47 C.F.R. § 64.7006), and one for other telecommunications carriers (47 C.F.R. § 64.2011). The Proposed Rules are similar. Unless otherwise specified, FTC staff's comments apply to both Proposed Rules.
[131] Health Breach Notification Rule, 74 Fed. Reg. at 42963.

actions suggested in the notification.[132] This data suggests that consumers may be overwhelmed by the volume of breach notices they receive.

FTC staff proposes two modifications to address these issues. First, as to BIAS providers, staff suggests that the notification requirement (but not the data security requirement) apply to a narrower subset of personal information than customer proprietary information and not include device identifiers, cookies, or other persistent identifiers standing alone.[133] Second, staff suggests including an exception to the notification requirement for certain inadvertent, good-faith actions by company employees that would otherwise meet the definition of "breach."[134]

Next, the NPRM asks how the FCC should treat data breaches by third parties with which a BIAS provider has shared information.[135] FTC staff suggests requiring BIAS providers to contractually obligate their agents to give the BIAS providers notice of breaches. The BIAS providers would then be required to provide breach notification to the affected consumers. This model ensures that the consumer would be receiving a breach notice from an entity with which the consumer has a pre-existing relationship, rather than a potentially unknown agent.

As to the timing of notice, the NPRM would require notice to the FCC and law enforcement within seven days, and to consumers within 10 days, subject to law enforcement needs.[136] FTC staff is concerned that this period for notice to consumers is too short and may

---

132 Ponemon Institute, *The Aftermath of a Data Breach: Consumer Sentiment* at 1, 5 (Apr. 2014), *available at* http://www.ponemon.org/local/upload/file/Consumer%20Study%20on%20Aftermath%20of%20a%20Breach%20FINAL%202.pdf.

133 While concerns about overnotification weigh in favor of excluding these categories from the breach notification, it is still very important that they be protected under the Proposed Rule's transparency, choice, and security provisions because these identifiers may be reasonably linked to a consumer, computer, or device. *See, e.g.*, Mobile Disclosures Report at 2.

134 *See, e.g.*, Health Breach Notification Rule, 74 Fed. Reg. at 42966.

135 Privacy NPRM, ¶ 237.

136 Privacy NPRM, Proposed Rule 47 C.F.R. §§ 64.2011, 64.7006.

not allow companies sufficient time to conduct an investigation. This could have a detrimental effect on consumers, who could get erroneous information about breaches. FTC staff suggests that companies be required to provide breach notice without unreasonable delay, but not later than an outer limit of between 30 and 60 days. Our experience suggests a limit in this range would be adequate for companies while protecting consumers. Additionally, FTC staff supports the requirement that any requests for law enforcement delay of notice to consumers be in writing and be effective for a finite period of time (which the relevant law enforcement agency could renew).[137] However, staff recommends requiring that law enforcement specify why the delay is needed. Although it is important that breach notification not interfere with law enforcement efforts, it is also important that consumers not be deprived of important information that helps to mitigate risks, unless law enforcement can articulate a good cause for delay.

Finally, as to contents of a breach notice, the proposed rule would require that the notices include contact information for the national credit reporting agencies.[138] While contacting the national credit reporting agencies may be appropriate in certain circumstances, it may not be helpful in others and could create a false sense of security. Credit reporting agencies maintain information regarding consumers' credit history, but not all breaches affect credit history. For example, if a consumer's email address is breached without more information, it is unlikely that this information can be used to open a new credit account in the consumer's name. On the other hand, some forms of fraud will not be captured by monitoring a credit report, including tax identity theft[139] or fraudulent charges on existing accounts.[140] FTC staff therefore recommends

[137] Privacy NPRM, Proposed Rule 47 C.F.R. §§ 64.2011(a)(3), 64.7006(a)(3).
[138] Privacy NPRM, Proposed Rule 47 C.F.R. §§ 64.2011(a)(2)(v), 64.7006(a)(2)(v).
[139] Tax and wage fraud was the largest category of consumer identity theft complaints in the FTC's Consumer Sentinel Network in 2015, at 45% of all identity theft complaints. FTC, *Consumer Sentinel Network Data Book for Jan. 2015 to Dec. 2015* at 12 (Feb. 2016), *available at* https://www.ftc.gov/reports/consumer-sentinel-network-data-book-january-december-2015.

that information about credit reporting agencies only be included in notices of breaches of information that can be used to open a new account – such as SSNs and financial account numbers. Staff also suggests requiring companies to include contact information for the FTC, and a reference to its comprehensive IdentityTheft.gov website. This website contains specific information about what consumers should do when they have received a breach notice.

## VIII. CONCLUSION

FTC staff supports the FCC's focus on the core privacy values of transparency, consumer choice, and data security. The suggestions provided in this comment are intended to strengthen the privacy protections that the FCC seeks to provide. FTC staff stands ready to provide further information and assistance as needed.

[140] For example, in the FTC's *Neovi* case, the company's Qchex product could be used to generate checks from consumers' bank accounts without their knowledge or consent, resulting in at least $402,750,000 in fraudulent withdrawals from consumers' existing bank accounts. *FTC v. Neovi, Inc.*, 604 F.3d 1150, 1154 (9th Cir. 2010).

**Summary of Staff Recommendations**

Defining "Personally Identifiable Information" ("PII")

- Define PII as information that is *reasonably* linked or linkable to a consumer *or a consumer's device(s)*
- Treat names, postal addresses, and phone numbers as PII

Privacy Notices

- Develop a standardized or model notice using consumer testing, use of which is a safe harbor for notice
- Translate privacy notice into the language the customer uses to transact business with the BIAS provider
- Require opt-in consent for material retroactive changes to privacy notices

Practices for Which Consent Is Implied

- To protect consumers from abusive family members, share PII in emergency situations only with family members the consumer designates
- Allow sharing of data needed to identify and trace abusive, unwanted, or illegal calls; the called consumer's number should be shared on an opt-out basis
- Ensure data is used only for the enumerated purposes that do not require consent, and no other

Practices That Require Choice

- Opt-in consent should be required for use and sharing of contents of consumer communications and sensitive data for purposes other than those for which consent is implied
- Opt-out is sufficient for use and sharing of non-sensitive data
- Under the sharing regime proposed by the NPRM, opt-out consent should be permitted for sharing of non-sensitive information with affiliates only where the affiliate is co-branded with the BIAS provider or the relationship is otherwise clear to the consumer; sharing with other affiliates should be permitted on the same basis as any other third-party

Present Choice at a Time That Is Relevant to the Consumer

- Choices should be unavoidable, short and simple, on their own separate screen, and easy to exercise
- Present choices at sign-up
- Give consumers access to and ability to select or change choices through a privacy dashboard

Data Security

- Require a written comprehensive information security program
- Require safe disposal of PII
- Develop robust security safe harbors with appropriate safeguards and enforcement

Breach Notification

- Provide notice for breach of a narrower set of PII
- Require third parties to report breaches to BIAS providers, and BIAS providers to provide the breach notification to consumers
- Require breach notification to consumers between 30 and 60 days after discovery of the breach
- Include information about consumer reporting agencies in breach notices only when relevant, and provide contact information for the FTC and the address of its IdentityTheft.gov website.