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.

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, sed [(TH)1(Ei)-2(on m)-2 EMC /Span <</MCID 24 >>B6C 12 0 0 0 8.04 278.732 Td 362.2(8)

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

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

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

consumers' ability to exercise choices.[25] And to promote strong data security practices, the FTC has brought approximately sixty enforcement actions

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.

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.a>per

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*

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,

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 statecnd

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 (A-pt..325 0v8 147(y) kd [(F)34(F)34(F)34(F)34(F)3 (e)-7.8(w)29.2(ad4(F)t)2.9(C)]T19.1(v)

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-

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]

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 (houl)h22 robocalls, but for all calls that a consumer identifTJ ies 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 (houl)h22 only calling pa]TJ ty phone numbers, but also any othe]TJ info]TJ mation these entities to locate or identifT-7(y)20( )-10(a)4(p)-10(h22)]TJ ticula]TJ 4(c)4(ons)-1(u

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-oPCi4(r(.-2ba)-6-16)-6-16ioboc3(al)

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 compasi0 T-1(r)3(e)-ng

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).

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

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 ifs2ateteWl TwT0.33 0 Td [(co)-4(m)-6(p) 0.004 T[atapn(el)

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 consotn(e)4(n)3(s)-1(sc)4(k)-10(em)lr/1amdi scm. 1oTc eparrryey dis

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

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

which largely mirrors the requirements contained in the order.[125] But, to ensur

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 "cou/ (76Tm ( )Tj 4-4(ur)3(pt Tc 0.j [("c)4(ou/(r)5(s 4B

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]

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

Summary of Staff Recommendations

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 xet6(s)]-2(f)0 Tw [(br)3(e)-6(0 Twbou.49 0TJ 0 T(h not)-2(i)-2(f)3(i)-2(c 0 Td [ie)6(a)4(c)4(