ESPC
Email Sender & Provider Coalition

February 17, 2011

Donald S. Clark
Secretary
Federal Trade Commission
Office of the Secretary
Room H-113 (Annex W)
600 Pennsylvania Ave., N.W.
Washington, DC 20580

Re: FTC File No. P095416: Comments of the Email Sender and Provider Coalition on the Preliminary Staff Report Entitled, *Protecting Consumer Privacy in a Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*

Dear Mr. Clark:

The Email Sender & Provider Coalition (ESPC) hereby submits these comments to assist Federal Trade Commission (FTC or Commission) Staff in its consideration of the appropriateness and feasibility of its proposed privacy framework (Proposed Framework). The ESPC appreciates the Staff's efforts to identify issues and potential solutions by inviting participation by all interested stakeholders. We look forward to a final report and framework that provide covered businesses with reasonable, practical ways to address real consumer concerns and with the guidance necessary to implement them.

Formed in November 2002, the ESPC's membership is comprised of many of the largest and most innovative technology providers in the email industry, including Email Service Providers ("ESPs"), Mail Transfer Agents, application and solution developers, and deliverability solutions providers. Members include Acxiom Digital, Constant Contact, Datran Media, e-Dialog, Eloqua, Epsilon, Responsys, Return Path, StrongMail, and SubscriberMail. For more information, please visit www.espcoalition.org.

The ESPC is made up of 54 leading companies. While email service providers serve the marketing needs of their clients, that is by no means the only customer group served. Email service providers also deliver transactional messages such as account statements, airline confirmations, purchase confirmations, email publications, affinity messages, and relational messages. They also provide clients with the tools to integrate with their other online marketing efforts.

The ESP industry is robust and growing. ESPC's clients represent the full breadth of the U.S. marketplace, from the largest multi-national corporations (indeed, the vast majority of Fortune 500) to the smallest local businesses (members of the ESPC serve hundreds of thousands of small businesses). Members of the ESPC also represent local schools, national non-profit groups, political campaigns, major publications with millions of subscribers, and small affinity-based newsletters. The use of ESPs by organizations large and small has become an industry standard.

I. Comments On The Scope Of The Proposed Framework

A. The Framework Should Exempt Service Providers From Its Coverage

As drafted, the Proposed Framework would apply to "all commercial entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer, or other device."[1] This definition is worded broadly enough to include entities that process data on behalf of and at the direction of a first party, with no right to use the data for their own or any other party's purposes (these are generally referred to as vendors or service providers). The Proposed Framework does not address its applicability to service providers. It should expressly exempt them from its privacy coverage.[2]

Not only would an exemption avoid the practical hurdles and inefficiencies associated with imposing the framework on service providers,[3] but there is also precedent for it. The Commission's Privacy of Consumer Financial Information Rule (Financial Privacy Rule), promulgated pursuant to the Gramm-Leach-Bliley Act,[4] also provides a template.[5] Congress did not make the Act's notice, choice, and related requirements directly applicable to service providers engaged by financial institutions, even though they receive and process sensitive financial data. Rather, as the Commission explains in its statement of basis and purpose for the final rule, the rule sets out the principle that "an individual should not be considered to be a consumer of an entity that is acting as agent for a financial institution. … [T]he financial institution that hires the agent is responsible for that agent's conduct in carrying out the agency

[1] Proposed Framework, p. 42.
[2] This is not to suggest that the ESPC believes that vendors bear no responsibility on information security. Quite to the contrary, the ESPC believes that all entities that maintain personally-identifiable information have a responsibility to safeguard it, consistent with the Commission's sliding scale approach that depends on factors such as on the nature of the data and the size of the company.
[3] For example, because service providers do not have their own relationship with consumers, it would not be feasible (nor would it make sense) for them to provide notice, choice, or access. The company with rights to the data is in the best position to comply, and this is what consumers would expect.
[4] 15 U.S.C. § 6801-6809.
[5] 16 C.F.R. § 313.

responsibilities."[6] The rule helps to ensure that the financial institution meets its responsibilities. Specifically, a financial institution may disclose a consumer's personal information to a third-party service provider, without giving the consumer the ability to opt out of that disclosure, as long as its privacy notice states that it makes such disclosures *and* it enters into a contractual agreement with the third party that prohibits it from disclosing or using the information other than to carry out the purposes for which it is disclosed.[7] The Commission determined that these protections were adequate for consumers' financial information.[8]

The same principles apply here, where less sensitive information is at issue. Accordingly, the ESPC respectfully requests that in its final report, the Commission exempt service providers from the framework's scope of privacy-related coverage.

B. The Framework Should Exempt Small Businesses From Its Coverage

The Proposed Framework is expansive: it effectively covers all commercial entities, whether operating online or offline, that collect or use consumer data. Coming into compliance with the framework's recommendations will present a challenge, as many of the anticipated recommendations do not reflect common U.S. business practices. For example, the "privacy-by-design" proposal would require a company to develop, implement, and enforce a comprehensive privacy program. As part of this, according to the Proposed Framework, a company would have to designate personnel to train employees, promote accountability within the company, and periodically review the program. This proposal would impose a new generally-applicable privacy requirement in the U.S. and, while laudable in theory, would, as a practical matter, impose substantial costs on businesses. It would require the hiring of qualified personnel to conduct not only an initial privacy audit but also regular, ongoing audits. Audits would have to be documented, adding another layer to the auditing and recordkeeping requirements with which companies already struggle. The burden of the framework's recommendations would be felt most acutely by small businesses that would not have the necessary personnel, technology, and other resources to come into and remain in compliance. We therefore urge the Commission to exempt small businesses from its final framework.

Members of Congress have considered this issue and favored such an exemption. On February 10, 2011, Rep. Bobby Rush (D-Ill.), former Chairman of the Subcommittee on Commerce, Trade and Consumer Protection, and current Member of the Subcommittee on Communications and Technology, released HR 611, a privacy bill intended to broadly regulate both online and offline

[6] Privacy of Consumer Financial Information; Final Rule, 65 Fed. Reg. 33646, 33651 (2000) (hereinafter, *Final Financial Privacy Rule*).
[7] 16 C.F.R. § 313.13(a).
[8] *Final Financial Privacy Rule* at 33670.

conduct. We understand that Rep. Rush's staff has spent many hours considering whether it would be appropriate to exempt small businesses from the bill's coverage, and ultimately decided that doing so would be appropriate. Specifically, it would exempt those persons that: (1) store covered information from or about fewer than 15,000 individuals; (2) collect covered information from or about fewer than 10,000 individuals during any 12-month period; (3) do not collect or store sensitive information; and (4) do not use covered information to study, monitor, or analyze the behavior of individuals as the person's primary business.9 The "discussion draft" released in May 2010 by Reps. Boucher (D-Va.) and Stearns (R-Fla.) contained a similar exemption.

Accordingly, in order to prevent an undue burden on small businesses – the drivers of the current recovery, especially in terms of job creation – the ESPC respectfully recommends that the final report include an exemption for them in the framework.

C. The Framework Should Exempt From Its Coverage Information Collected And Used In A Business Context

The Staff defines the scope of the Proposed Framework as "all commercial entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer, or other device."[10] The inclusion of the word "consumer" makes it reasonable to assume that the Staff intends the framework to apply only to information obtained from an individual in the context of a consumer interaction (*i.e.*, one primarily for personal, family, or household purposes); however, this is not completely clear. We therefore urge the Commission to expressly exempt from the framework's scope information collected from or about an individual in his or her capacity as a representative of a business and used in the context of a business-to-business relationship. The burden should be on the data collector (not the individual) to establish that a particular context is business-to-business.

An exemption for business information is appropriate. The protections contained in the Proposed Framework are not necessary for business contact and related information. In the business context, individuals have less of an expectation of privacy because the information collected from and about them does not pertain to their personal, home, or family lives. When business contact information is used for legitimate business purposes, the information poses little or no risk of identity theft or of intrusion into an individual's private life. Moreover, individuals acting in their professional capacity, and their employers, typically expect and want their information to be shared easily with others. Imposing, for example, the same notice and consent

[9] Sec. 2(3)(B).
[10] Proposed Framework, p. 41.

obligations as those that apply to consumer data restricts the collection and sharing of such information and, as a result, hampers efficiency.

Rep. Rush's privacy bill, the BEST PRACTICES Act, also contains an exemption for business information. It expressly excludes the following from its definition of "covered information": "the title, business address, business email address, business telephone number, or business fax number associated with an individual's status as an employee of an organization, or an individual's name when collected, stored, used, or disclosed in connection with such employment status."[11]

There is also Commission precedent for exempting business information from the framework. Commenters to the proposed Financial Privacy Rule asked that transactions that fit within the business, commercial, and agricultural exemptions from the Truth in Lending Act and its implementing Regulation Z, be treated as beyond the scope of the rule.[12] In its statement of basis and purpose for the final rule, the Commission agreed with them, without explanation.[13] It revised the final rule to apply "only to nonpublic personal information about individuals who obtain financial products or services primarily for personal, family or household purposes from the [covered] institutions. This [rule] does not apply to information about companies or about individuals who obtain financial products or services for business, commercial, or agricultural purposes."[14] If the Commission believed it appropriate to exempt business-related financial information from the protections provided by its Financial Privacy Rule, then it seems similarly – if not even more – appropriate to exempt business-related personal information from the final framework. We respectfully request that it do so.

[11] Sec. 2(4)(B)(i).
[12] *Final Financial Privacy Rule* at 33648. Those provisions exempt from the coverage of the Act and Regulation: "[c]redit transactions involving extensions of credit primarily for business, commercial, or agricultural purposes, or to government or governmental agencies or instrumentalities, or to organizations." 15 U.S.C. § 1603(1), 12 CFR 226.3(a).
[13] *Final Financial Privacy Rule* at 33648.
[14] 16 C.F.R. § 313.1(b). The exclusion of business information is repeated in the rule's definition of a "consumer" (which definition essentially triggers the rule's requirements): "an individual who obtains or has obtained a financial product or service from [a covered financial institution] that is to be used primarily for personal, family, or household purposes." 16 C.F.R. § 313.3(e)(1). The Fair Credit Reporting Act similarly limits its scope to consumer information by defining a "consumer report" in relevant part as a communication of certain information by a consumer reporting agency "which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for credit or insurance to be used primarily for personal, family, or household purposes." 15 U.S.C. § 1681a(d)(1)(A).

II. Comments On Simplified Choice

A. The Proposed Framework's "Commonly Accepted" Paradigm Needs Further Analysis

The Proposed Framework encourages companies to take steps to simplify consumer choice. Specifically, the Staff proposes a bifurcated approach that (1) permits companies to infer consumer consent to data uses and disclosures that are "commonly accepted," and (2) requires them to obtain meaningful consent for uses and disclosures that do not fit within the narrow category of "commonly accepted" uses and disclosures.

The proposal presents a striking new obligation for businesses, yet the Staff has presented it without any record of analysis of the effect that its imposition would have on businesses. The Staff notes that, "under current law, many companies are not required to provide – and do not currently provide – choice to consumers."[15] It goes on to explain that its goal in proposing a streamlined choice model "is to foster clearer expectations for consumers and businesses regarding the types of practices for which choice should be provided."[16]

Apart from a desire to provide consumers with a simplified way to exercise control over their data, however, it is not clear how or why the Staff decided that businesses should provide consumers with choices with respect to "not commonly accepted" data practices. The Staff appears to have proposed this "recommendation" as a remedy to consumers' perceived lack of choice, but the Staff request does not even request comments on the effects that this proposal would have on online and offline commerce.[17] The proposal's potential costs, as well as its likely disruptions to efficient data flows and stifling effect on innovation, are likely to be significant,[18] and they warrant a robust review – including participation by all interested stakeholders – before the Staff finalizes this recommended standard. ESPC may well support

[15] Proposed Framework, p. 53.
[16] *Id.*
[17] Instead, the Staff requests comments on the practices that should or should not be designated as "commonly accepted," as well as on how businesses should obtain consent for practices that are not so designated.
[18] Consider, for example, the cross-channel processes that businesses will have to adopt to ensure that consumers are given the opportunity to consent to various data uses. A company that runs an offline loyalty card program, for example, will have to print new notices and ensure that they are distributed to potential members. Moreover, businesses will have to build systems and databases that are capable of ensuring that consumer choices are appropriately recorded and honored, even as they may change from time to time. Finally, employees will have to be trained around all of these processes.

such a framework, or one like it, but respectfully comments that it cannot do so until the Commission has engaged in such a review.[19]

B. The Use Of A Service Provider Should Always Be Considered A "Commonly Accepted" Practice

As noted above, the Proposed Framework calls on companies to simplify the choices that they offer consumers about how their personal information is used and disclosed. To that end, the Staff proposes that companies not be required to seek consent for certain data uses and disclosures that are "commonly accepted" by consumers, as such a requirement would "impose significantly more burden than benefit on both consumers and businesses."[20] This is also true, according to the Staff, where companies use service providers to process consumer information in connection with the "commonly accepted" uses, provided that there is no further use of the data by the service provider.[21]

If the Commission retains this proposal, then the Staff's inclusion of service providers in the category of "commonly accepted" practices is important, but it does not go far enough. The underlying data use performed by a service provider may or may not be "commonly accepted"; however, the fact that a first party may use a vendor to perform a task it could do itself but chooses for purposes of efficiency to delegate, is. Consumers understand and expect that companies use vendors for various functions. Accordingly, when a company is required to provide a consumer with choice with respect to a "not commonly accepted" use of his or her information, it should not have to also provide the consumer with a choice with respect to whether it uses a service provider to process his or her data in connection with that use. To impose such a requirement would incent companies *not* to use service providers for "not commonly accepted" uses of personal data. It could also result in inefficiencies, a disincentive to innovate, and a decision against offering products, services, or features that may benefit consumers. For these reasons, if the Commission retains its "commonly accepted" theory in its final framework, then at least one of these practices should be the processing done by service providers.

There is Commission precedent for treating the use of service providers, regardless of the nature of the data processing they provide, as "commonly accepted" and therefore not subject to

[19] The "commonly accepted" framework also suffers from inherent vagueness. What is and is not commonly accepted is subjective to the individual and the circumstance, and will also change over time as technology and business models – and consumers' experiences – change.

[20] Subject to the Staff's review of the comments it receives, the "commonly accepted" uses and disclosures are limited to those that fall within the following five categories: product and service fulfillment; internal operations; fraud prevention; legal compliance and public purpose; and first-party marketing. Proposed Framework, p. 53-54.

[21] *Id.* at 54-55.

consumer choice. The Financial Privacy Rule generally requires a financial institution to give its consumers the ability to opt out of its sharing of their personal information with non-affiliated third parties. There is an exception for service providers: although a financial institution must provide consumers with notice of its sharing of their personal information with service providers, it does not have to give them the ability to opt out of such sharing.[22] The Commission determined that this approach provided consumers with sufficient control over their sensitive financial information. It should take the same approach here.

C. First Party Marketing, Including The Delivery Of Retargeting Emails, Should Be Exempt From the Commission's Do Not Track Proposal

The Proposed Framework includes the Staff's support for a do not track mechanism for online behavioral advertising, but it does not define "online behavioral advertising." We urge the Commission to define the practice to expressly exclude "first party" advertising, where no data is shared with third parties other than service providers, as it did in its 2009 Self-Regulatory Principles for Online Behavioral Advertising.[23] We further urge the Commission to expressly include the delivery of retargeting emails, and its attendant analytics and reporting,[24] within its definition of "first party" advertising. A retargeting email is delivered to a site visitor based solely on his or her visit to a particular site and may include, for example, the promotion of a product based on his or her prior purchases or browsing activities *at that site*.[25] The Staff's own explanation for why first party advertising should not be regulated as online behavioral advertising applies equally to retargeting email:

> [S]taff agrees [with commenters] that "first party" behavioral advertising practices are more likely to be consistent with consumer expectations, and less likely to lead to consumer harm, than practices involving the sharing of data with third parties or across multiple websites. For example, under the "first party" model, a consumer visiting an online retailer's website may receive a recommendation for a product based upon the consumer's prior purchases or browsing activities at that site . . . In such case, the tracking of the consumer's online activities in order to deliver a recommendation or

[22] 16 C.F.R. § 313.13(a).

[23] *FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising* (2009) (hereinafter *OBA Report*), www.ftc.gov/os/2009/02/P0085400behavadreport.pdf. In the report, the Staff concluded that first party behavioral advertising practices "are more likely to be consistent with consumer expectations, and less likely to lead to consumer harm, than practices involving the sharing of data with third parties or across multiple websites." *Id.* at 26.

[24] Email delivery analytics and reporting permit email marketers to understand deliverability, open rates, and other measures of their campaigns' efficacy. Without them, the market would be inefficient.

[25] Of course, any retargeting email, the primary purpose of which is commercial, would be subject to the requirements of the CAN-SPAM Act, including its prohibition on sending commercial email to a person who has previously opted out of receiving it.

advertisement tailored to the consumer's inferred interests involves a single website where the consumer has previously purchased or looked at items. Staff believes that, given the direct relationship between the consumer and the website, the consumer is likely to understand why he has received the targeted recommendation or advertisement and indeed may expect it. The direct relationship also puts the consumer in a better position to raise any concerns he has about the collection and use of his data, exercise any choices offered by the website, or avoid the practice altogether by taking his business elsewhere. By contrast, when behavioral advertising involves the sharing of data with ad networks or other third parties, the consumer may not understand why he has received ads from unknown marketers based on his activities at an assortment of previously visited websites. Moreover, he may not know whom to contact to register his concerns or how to avoid the practice.[26]

It does not matter whether the advertiser itself delivers the retargeting email or whether a service provider does so on its behalf. In the OBA Report, the Staff concluded that sharing with service providers for the purposes of first party advertising is still considered first party use, provided that there is no further use of the data by the service provider.[27]

D. Use Of A Do Not Track Mechanism Should Not Opt Consumers Out Of Email Marketing

If the Commission continues to support a do not track mechanism for online behavioral advertising in the final framework, we urge it to work with those developing industry or self-regulatory mechanisms and/or policymakers to ensure that the choice expressed via any such mechanism is understood and implemented as solely that: a choice not to be tracked online for purposes of online behavioral advertising. It should not be interpreted more broadly, to imply that the consumer does not want to receive *any* targeted or direct marketing, including but not limited to commercial email.

Businesses offer consumers different ways in which to express their choices to initiate and/or stop the receipt of various forms of targeted and direct marketing. (Many of these are, of course, compelled by laws and rules enforced by the Commission.) To interpret a "do not track" choice more broadly than intended would risk thwarting consumers' expressed choices and undermining the effective consent mechanisms already in place.[28] Accordingly, to avoid uncertainty in the

[26] *OBA Report* at 26-27.
[27] *Id.*, note 58.
[28] In any event, such a requirement would be technically impossible, at least under the Commission's suggested methodology involving the setting of a persistent cookie in a browser, because email readers are not web browsers and have no ability to read or retain information expressed in a cookie. This means that they could not react to any preference expressed in a browser.

final report, we request that the Commission make it clear that a choice not to be tracked online for purposes of online behavioral advertising does not extend to any other form of direct marketing.

III. Other Comments

A. The Framework Should Incorporate The Concept Of Distributed Compliance

We urge the Commission to incorporate within any final framework the concept of "distributed compliance." What we mean by this is that a covered entity should be able to rely on the representations and warranties (with respect to framework compliance) of any other covered entity from which it receives consumer data for its own use. This assumes, of course, proper monitoring of some kind to make sure that the entity from which the data were acquired complies with the framework. Without support for this concept, the framework takes on the form of strict liability for everyone that touches data used for a specific purpose. There is no better way to stifle innovation that to impose liability in this way; it will chill the market from new, innovative, efficient, and economically beneficial ways of using data. Moreover, it would be extremely difficult and costly for one company to determine via due diligence efforts whether another company is in compliance with the framework. Not only could it not do so itself, but, unlike in the data security arena, there is not currently a well established market of vendors available and qualified to evaluate privacy compliance.

B. The Commission Should Add A Step To This Process

In its introduction to the Proposed Framework, the Staff explains that the "framework is designed to serve as a forward-looking policy vehicle for approaching privacy in light of new practices and business models. However, it incorporates elements that reflect longstanding FTC law."[29] By way of example, the Staff cites to: (1) enforcement actions the Commission has brought under Section 5 of the FTC Act, alleging companies' failures to take reasonable steps to secure consumer data; and (2) the Section 5 unfairness action that the Commission brought against Gateway Learning, challenging the company's allegedly retroactive application of a material change to its privacy policy. Although these examples are helpful in that they identify parts of the Proposed Framework that the Commission believes it can uphold pursuant to its Section 5 authority, they are presented as examples only. It is not clear from the Proposed Framework or the preliminary Staff report accompanying it which additional provisions of the Proposed Framework (if any) the Commission would consider to be actionable under Section 5, and which are only intended to guide Congress, other policymakers, and industry as they develop legislation and/or self-regulatory guidelines or best practices. In particular, the Staff's repeated

[29] Proposed Framework, p. 39.

use of the word "should" in connection with its proposals[30] makes it reasonable to conclude that the proposals themselves do not impose legal obligations on businesses; however, stronger language is used in the descriptions of certain proposals. For instance, in its discussion of simplified choice, the Staff states that, with respect to all "not commonly accepted" data practices, "the framework would *require* companies to give consumers the ability to make informed and meaningful choices."[31] (emphasis added) In other places in the same section, the word "should," rather than "require," is used. Without further guidance, industry has no meaningful way to prioritize how to come into compliance with the various framework provisions. The guidance should not have to come, in the first instance, through an enforcement action.[32]

To provide the needed clarity, we urge the Commission to add an interim final report to its review and implementation process, identifying which parts of the framework it considers required by Section 5 and which are intended as best practices and/or are provided for legislative and/or self-regulatory consideration. Interested stakeholders should be given the opportunity to comment on the interim report before it is finalized. Without such transparency, industry will be left not knowing which parts of the framework are enforceable and which are aspirational – a result that would render the entire process less useful to the market than it could be, and, therefore, less likely to achieve the Commission's goals.

* * *

[30] Except for its statement that "[c]ompanies *must* provide prominent disclosures and obtain affirmative express consent before using consumer data in a materially different manner than claimed when the data was collected." *Id.* at 76. (emphasis added)

[31] *Id.* at 57.

[32] In its Executive Summary to its preliminary report issued with the Proposed Framework, the Staff states that, in the interim period before it issues a final framework (*i.e.*, while it accepts and reviews comments and then drafts the final framework), "the Commission plans to continue its vigorous law enforcement in the privacy area, using its existing authority under Section 5 of the Federal Trade Commission Act and the other consumer privacy laws it enforces." *Id.* at p. viii.

The ESPC appreciates the opportunity to comment on this important initiative and looks forward to continuing to work with the Staff and other stakeholders to develop an appropriate privacy framework.

Respectfully submitted,

D. Reed Freeman, Jr., Esq.
Outside Counsel, Email Sender and Provider Coalition

Morrison & Foerster LLP
2000 Pennsylvania Avenue, NW, Suite 6000
Washington, DC 20006
202.887.6948
rfreeman@mofo.com

cc: ESPC Board of Directors
ESPC Members