Baker Hostetler

Baker&Hostetler LLP
Washington Square, Suite 1100
1050 Connecticut Avenue, N.W.
Washington, DC 20036-5304
T 202.861.1500
F 202.861.1783
www.bakerlaw.com

Barry J. Cutler
direct dial: 202.861.1572
BCutler@bakerlaw.com

February 18, 2011

VIA ELECTRONIC MAIL AND HAND DELIVERY

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

Re: Comments on the Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change - FTC File No.P095416

Dear Secretary Clark:

I submit this comment on behalf of the Electronic Retailing Association ("ERA") in response to the Commission's invitation regarding the Preliminary Staff Report on Protecting Consumer Privacy. Please note that this comment supplements ERA's views that are contained in a submission by a coalition of associations and companies that are interested in this subject matter.

The ERA is a leading trade association in the U.S. and international markets that represents leaders in the direct to consumer marketplace. The members maximize revenues through electronic retailing utilizing the television, internet and radio. ERA strives to work with regulators and legislators to create a climate that ensures a favorable landscape that enhances e-retailers' ability to bring quality products and services to consumers in this $300 billion marketplace. ERA represents over 450 companies in 45 countries with membership consisting of e-commerce companies,

traditional advertisers, home shopping networks, direct response marketers and associated supplier categories including call centers, fulfillment companies, international distributors and payment processors. Member companies include some of the world's most prominent retail merchants, including Allstar Products Group, eBay, Discovery Communications, Gaim, Google, Guthy-Renker, HSN, Oak Lawn Marketing, Product Partners, QVC, Telebrands, ShopNBC and Thane.

Not only does the ERA advocate a self-regulation approach in this comment, but it has for several years sponsored a successful advertising self-regulation program, known as the ERSP, that is run under the auspices of the National Advertising Review Counsel ("NARC") of the BBB. ERA is committed to making self-regulation work wherever it can provide a more efficient and flexible vehicle for industry compliance than formal government rulemaking.

OVERVIEW

The ERA has focused on a high level discussion that it believes is required to give the FTC a context to consider the responses it will get to the many questions it published in the Federal Register. We offer a set of "first principles" that are derived from prior FTC rulemaking efforts--some very successful; others less so. Specifically, we use the first principles to answer many of the specific questions the FTC has raised.

FIRST PRINCIPLES

There are five "first principles" that the FTC would do well to consider to inform its judgment about the next or a final proposal. They are:

- **Particularly where technology and the methods of passing and capturing personal information are changing every month or two, industry self-regulation, with frequent collaboration with government, is a far superior platform for mid-course corrections than Rules or Guides that require Section 553 rulemaking.**

- **Providing Guides or a "Best Practices" List will get better compliance results than a Regulatory Standard because some flexibility in approach is more effective for dealing with privacy than a "one-size-fits-all" Rule.**

- **If Rules are adopted, they must be designed to benefit consumers rather than make for easy FTC enforcement.**

- **Rules Should Reflect Performance Standards, Not Design Standards.**

- **Because not all concerns about marketing data are of equal weight, the FTC should consider costs and benefits of proposals, including whether a Rule is needed in the first place for a particular issue.**

A. Industry self-regulation, with frequent collaboration with government, is a far superior platform for mid-course corrections than Rules or Guides that require Section 553 rulemaking.

When the Commission announced its Mail Order TRR in the summer of 1975, it recognized that the use of telephones to place orders was growing rapidly and might even pass the Postal Service for delivering orders otherwise governed by the Rule. The Commission demurred from expanding the new Rule because the rulemaking procedure was cumbersome and there was not yet enough data to support the need for a rule. It waited nearly two decades to expand what is now the Mail and Telephone Order TRR.

When the Commission announced its Telephone Sales Rule ("TSR") in 1995, online sales over the internet was in its infancy. Over the next five to ten years, online sales of goods and services grew dramatically. According to the most recent Annual Reports of the Commission, complaints about internet fraud and deception and other internet-related complaints constituted about two-thirds of consumer complaints to the Commission. Virtually none of these complaints were an issue when the Commission first passed the TRR. Even with the less formal procedures of 5 U.S.C.

§ 553, the Commission has not gone back to amend the Rule to provide a comprehensive Rule for internet sales.

By comparison with Mail Order and Telemarketing sales, the issues and technology that are salient to privacy do not change over years, but over months or weeks. New apps, new tracking and aggregating techniques, new forms of social networking can present questions like those the Commission asks in Appendix A.

If the Commission were to propose a rule with bright-line standards, it is hard to predict with confidence that it would not have serious gaps several weeks or months after. Indeed, in the time it takes to complete even Section 553 rulemaking, it is not likely that the evidentiary record would be adequate to deal with new issues that arose over the course of the proceeding.

On the other hand, if the Commission were to enact more flexible rules that are broad enough to cover new developments as they arise, the Rule would necessarily be too imprecise to permit widespread enforcement without chaos for businesses trying to comply.

None of these issues would cause great concern unless the Commission's main focus is publishing a regulatory scheme that will be easy to enforce, especially against those who abuse private and confidential information. See Section C, below. Not only would such a Rule risk the obsolescence stated above, but it would prove particularly burdensome on legitimate businesses that would try hard to comply with specific and ill-fitting rules.

Some of the trade associations submitting comments in this proceeding have sponsored or participated in self-regulation activities with considerable success. ERA itself has its own advertising program, the ERSP, that is administered by the BBB/NAD as an adjunct to the regular NAD process. The Direct Marketing Association ("DMA") has internal standards that it enforces against members who are expected to comply with them.

At least until the Privacy issue progresses to the point where clear standards emerge for topics such as "commonly

accepted practices" and the like, industry self regulation has many benefits, including the commitment of many mainstream marketers to follow the standards they adopt and a platform that can accommodate rapid changes in the marketplace more easily than A.P.A. rulemaking can.

Self-regulation does not mean hanging up a sign that says "Government Stay Away." Effective self-regulation should include considerable interaction between sellers and the government in which the government can explain the standards of protection it thinks are desirable and the industry can help the Commission distinguish between abusive practices versus general practices used by legitimate as well as abusive marketers. See Section C, below.

Whether or not a time may come where there is adequate information to promulgate a formal Privacy Rule, this surely is not that time. By working with industry on a cooperative basis, the Commission can avoid the twin evils of too much specificity and too much generality. The Commission should not issue a Rule for privacy before attempting to facilitate a rigorous but reasonable self-regulation program with wide industry support.

B. Providing Guides or a "Best Practices" List will get better compliance results than a Regulatory Standard because some flexibility in approach is more effective for dealing with privacy than a "one-size-fits-all" Rule.

Although ERA believes that a self-regulation approach is the best at this time, it is not the only way to avoid a rule that will stifle innovation and frustrate companies that are trying to comply in good faith. The FTC has issued Guides that have successfully given guidance to companies without burdensome and unnecessary rigidity.

One good example is the FTC's Green Guides, first issued in 1992 with general support of the business community, the state attorneys general, and environmental groups. As the Commission well knows, it achieved this consensus by issuing general guidance coupled with specific examples that afforded advertisers and their counsel a fair comfort level about the compliance of claims they were working on.

To be sure, the Commission is engaged in a revision of those Guides at this time. However, it is not because "old" notions have become obsolete or irrelevant, but because new concepts and popular phrases have arisen. "Sustainable" is a good example. Although the Commission is working on these newer concepts that need some guidance as to appropriate meaning and scope, almost all of the original Guides have passed the test of time well. This is clear from the Commission's Federal Register notice that left so much of the original Guides intact, sometimes by retaining the Guide but updating it with a couple of fresh examples.

Another more recent example is the Commission's handling of the Red Flags Rule for ID theft prevention and detection. As with privacy, the role of the various red flags varies greatly among the many very different types of creditors. The variations in the sensitivity of data companies capture, what they use it for, and how long they retain it, is subject to infinite variations.

The Commission selected a very flexible approach that would not dictate the final Program of any creditor. Specifically:

- The Commission selected 26 factors that each creditor should consider, picking those that were relevant to their respective businesses.

- Creditors were free to consider other factors that might apply to their circumstances.

- The Commission made clear that small businesses, or others for whom the risk of involvement in ID theft was quite low, could plan a truncated Program suitable for their circumstances.

- While giving a wide berth for compliance content, the Commission required that the Board of each company, or a suitably engaged executive, would be responsible for making sure that the process for developing a Program was taken seriously.

To borrow a phrase from the current proposal, the Commission adopted an "ID Theft Prevention by Design" approach. Quite literally, each program was tailored to the situation of the company.

Privacy concerns are as varied as Red Flags concerns. If the Commission truly wants to facilitate a "privacy by design" approach, it needs to create a similarly flexible program for companies to follow. The alternative of a rigid approach is a Privacy by FTC Design theme, obviously not destined to maximize the benefits of each program.

This "first principle" ties into the prior one. The fact that technology and opportunities to capture personal information will change quickly makes flexibility critical. The annual review for ID Theft programs makes a good analogy for what is needed for privacy. A Rule that is "set in concrete" will prevent the ongoing benefits of a flexible policy.

With this overview in mind, several of the FTC's Questions in Appendix A can be addressed using this first principle.

a. G1:[1] Why would FTC want to "standardize the format and terminology" for data practices across industries, given the variations among industry members? As with terms in the Truth in Lending Act ("APR") or the Magnuson-Moss Warranty Act ("Limited Warranty"), there likely are some basic terms in the Privacy rubric, such as "personally identifiable information," for which uniform terminology could have some benefits. But a more broadly based "standardized format and terminology" requirement makes no more sense than it would to require a standardized format for privacy policies.

---

1 The FTC did not use a letter or numbering system for the questions in its Appendix A. For ease of reference, we have "lettered" the main headings and "numbered" the bulleted subheadings and attach a copy of Appendix A annotated with the letters and numbers we have assigned. For example, "G1" refers to the question about using "standardized format and terminology."

b. G3: What benefit is expected by mandating terms be "Machine readable to allow" comparisons of privacy practices? For TILA disclosures, comparisons make sense. For many other consumer goods, however, there is very little evidence that consumers compare, e.g., warranty terms as a material guide to purchases, even with the Pre-Sale Availability Rule. Law enforcers and academics are much more likely to want to compare privacy practices than consumers are. See Principle C, below. Such a requirement would carry costs for small and large businesses alike, without much benefit to consumers.

c. G9: Before considering "standardized means for providing consumer access," the Commission must consider how necessary widespread access is in the first place. This topic deals, for the most part, with marketing data, not FCRA data or medical data. Where data is specifically covered by laws such as the FCRA or HIPAA, the statute provides the "uniform" means as needed. To set uniform means for access to routine consumer data used commercially—for all data and all types of businesses—seems quite inconsistent with "Privacy by Design."

d. F9: Particularly in a regulatory mode rather than in Guides or a list of best practices, how could the FTC provide specifics for more across the board "granular control" by consumers over specific types of ads or types of information. By comparison with scrubbing a list of phone numbers against the National Registry, it would seem chaotic for sellers to have to maintain and apply the random wants of individual consumers as to messages they receive.

e. D1: The example of "commonly accepted practices" provides the best analogy to Red Flags. As guidance or in a list of best practices, some indicia of "commonly accepted" could be helpful without concern for whether the term is defined too narrowly or too broadly. To seek clarity in a regulatory environment seems fraught with the danger of missing the flexibility that is needed on such an overarching issue.

f. B3: It is simply hard to imagine that there could be a one-size-fits-all retention policy for all types of businesses and all types of data. Nor is there any apparent need to do so.

g. B4: Proposing that a retention period be based on "sensitivity of data" ignores the reality that businesses often have multiple purposes for information---not just behavioral advertising. It is more important to influence what companies DO with their data than how long they retain it. This is not to suggest that it would be ill-advised to have "best practices" suggestions to help companies decide how long they really need to keep data.

h. B5: Likewise, it seems implausible that all "legacy data systems" can be treated similarly and there is no plausible reason it is necessary to do so.

i. A3: The idea that an enforceable regulatory standard could apply to the different ways that information could become "linkable" in the future is a fantasy. The Commission could put out some guidance on the question, but it could not reasonably govern events that have not happened yet and that are totally unpredictable.

C. Rules must be designed to provide Consumer benefits rather than for making enforcement easier for government.

It is not uncommon for law enforcers to draft rules that are of little benefit in actual practice, but make it easier to "detect" violations in a compliance investigation. This tendency may be intentional in some cases, inadvertent in others.

A good example comes from the requirement in the FTC's Funeral Practice Rule that funeral directors must disclose at the outset of a phone conversation that price information is available to the caller. The funeral industry long has considered the rule awkward and, often, offensive to consumers who call at a difficult time and are bombarded, it

seems, with an unsolicited offer of pricing information. An important reason for the provision was that it was easy for investigators in a "sweep" to determine if directors were complying by phone.

Another example was an element of the initial proposal of the Telephone Sales Rule, which was intended (and later changed) to identify and stop practices that fraudulent telemarketers used. One of them was prohibiting the use of "desk names," an alias for the telephone rep. While most fraudulent telemarketers did use desk names, it turned out that many legitimate firms, even public interest NGO's, used the same practice to protect their employees. The provision was dropped during the rulemaking proceeding with the result that all telemarketing firms were not saddled with a requirement that did not actually target the "bad guys." The requirement would have made it easy to discern violations.

For many practices listed in the FTC's Appendix A, uniform practices and definitions and one-size-fits-all requirements that would be easy to investigate for violations will unlikely prove flexible enough to survive changes in practices for technology or other reasons and provide benefits to consumers.

D. Rules Should Reflect Performance Standards, Not Design Standards.

Other than to point to this "first principle" and cite an example or two, little elaboration is needed. In other aspects of its work, the Commission has recognized and advocated "performance standards" (how a product or practice works) rather than dictate "design standards" (actual specifications). While there are periodic exceptions for special circumstances, *e.g.*, strict fencing in is needed, the Commission has been strong on this issue.

One clear example is the "clear and conspicuous" requirements for disclosures. In most cases, the Commission uses a definition in terms of "legible and understandable" rather than dictating type-size and other design attributes.

A second example is the Commission's Green Advertising Guides, in which the Commission rejected public comments to

require a minimum amount of post-consumer waste for a product to be called "recycled." Rather, the Commission required a clear disclosure of the amount of post-consumer waste—be it 10 percent or 50 percent—and left it to competition to respond to consumer wishes and needs. While not really a "performance" standard, the Commission's choice was an excellent example of avoiding a restrictive design standard.

Perhaps the best example is one that raises both consumer protection and antitrust concerns—work the Commission has done over the years for private standards setting and certification. If two products are capable of meeting a performance standard, a standards organization risks liability if it unjustifiably requires one product over the other. Copper versus PVC pipes for construction is one example. Environmental certification programs that automatically approve paper over plastic when both can safely meet a performance standard runs a similar risk.

It is not difficult to apply this first principle to some of the FTC questions.

a. F3: The FTC asks about how to make a Do Not Track mechanism "clear, easy-to-find, usable, and understandable." The FTC should not dictate a rigid disclosure, but provide criteria that, like "clear and conspicuous," would make a mechanism both flexible and effective.

b. E1: The question asks the "most appropriate way" to obtain consent for practices that are not "commonly accepted." ERA joins others in urging that such questions be answered by an "opt out" rather than an "opt in" approach. Even with an opt out procedure, however, the Commission should not assume that any option is needed in every case.

Some issues in the advertising milieu, unlike credit and health, raise sufficiently trivial issues of privacy that the extra work to implement an option protocol is not justified. This point provides a segue to the next first principle about weighing costs and benefits. In any event, in instances where the Commission thinks an option approach is needed, it should follow the Red Flags model and allow firms to devise

solutions that are effective in their context, not dictate a set of specifications that may not be useful across different situations or as times change.

This principle also ties into the top points about self regulation and flexibility. In an area that is changing as quickly as privacy, the Commission should be skeptical of any design standard that could be superseded by new technology but still be stuck in a Rule that would stifle progress.

E. Essential to Consider Costs and Benefits in Complicated, Changing Market.

The first question for many of the questions under consideration should be "is this necessary in the first place?" Do the costs outweigh the benefits or vice versa? Although the Commission has a good record on costs versus benefits, several of the questions in Appendix A do not explicitly suggest that such a question will be asked.

A example from 40 years ago demonstrates this principle in the context of privacy. When the Fair Credit Reporting Act ("FCRA") was relatively new and not widely construed, the Commission had to deal with the question of "prescreening" and "firm offers of credit." In a policy statement, the Commission determined that prescreening was appropriate when certain conditions were met. For years after, scholars and advocacy groups argued that the practice was not really permitted by the plain meaning of the Act. The Commission, however, determined that the "trivial" effect on privacy was outweighed by the efficiency of firm offers of credit.

We understand that the law was changed more recently when the Congress determined to allow prescreening, but offered consumers a choice. The facts remain, however, that the cost benefit analysis worked for more than 30 years and, when it was changed, the Congress itself went with an opt out provision rather than an unwieldy opt in one.

Issues of costs and benefits still abound, even in the Commission's questions.

a. E3: Under what circumstances is it appropriate to make an option "take it or leave it?"

It is likely that a majority of the rules consumers encounter in their everyday lives are offered on a 'take it or leave it" basis. The standard Privacy Policy is a good example. Consumers are told, in effect, to read the Policy and, if they are not comfortable with it, they should not leave personally identifiable info on the site.

A related example occurs in the blogosphere, when some hosts require a commenter to provide a name and a working email address. As with many other privacy issues, the burden and inefficiency of giving bloggers an option to leave a name and email address or not greatly outweighs the benefit, which is simply allowing a blogger to add his or her thoughts to a list of web comments.

As with other privacy practices, the Commission should not start with a negative presumption about the issue of "take it or leave it." Perhaps the Commission did not do so, but there is little in the question, as asked, that suggests that a cost benefit inquiry is appropriate. The costs of making individual exceptions or prohibiting some take it or leave it options could be cost prohibitive and/or a compliance nightmare.

The Commission might find some small number of instances where "take it or leave it" could be unfair or burdensome. If a service is indispensable as a practical matter and the privacy practices more obtrusive than necessary, it should be possible to describe factors that warrant an exception on a narrow basis.

In some areas, such as children's online information (COPPA) or health information (HIPAA), privacy concerns triggered federal laws to prescribe the limits and the requirements of gathering personal information. These are special exceptions to normal everyday privacy issues. The Commission should not, as it sometimes implies, assume that a "choice" or "access" to information is critical in a marketing context.

b. E4: If the Commission can identify circumstances where "take it or leave it" is inappropriate, a limited carve out should be created. Otherwise, the FTC should not impose costs in the types of situations in which consumers face "take it or leave it" choices in their everyday lives.

c. F5: The Commission does ask about costs and benefits for a standardized uniform choice for Do Not Track (behavioral advertising). The answer is: it depends. First, one must consider whether there is an inexpensive technological mechanism, such as a cookie-like device, or only a cumbersome and expensive mechanism, such as a National Registry, which has worked for telephone calls, but would be much more expensive and inflexible for behavioral advertising.

After all, the "Do Not Track" option does not prohibit pop-up ads or emails of a commercial sort. It excludes, ironically, only those ads that may be most attractive to consumers because they were selected by cues as to his or her interests. In any event, a technological solution may come along that will let consumers make the choices via a computer's settings, thereby taking the seller out of the picture and without incurring a heavy administrative cost.

d. E7: The Commission shows special interest in teens, particularly in the context of social networking. This issue ties together many of the "first principles" we have been discussing.

The issue of social networking will continue to receive great attention and is a serious social issue. Where Congress thought regulation was needed, it passed COPPA. For other situations, more progress is likely to come from voluntary efforts and experimentation (best practices) rather than a rigid regulatory solution (rules) for a diverse and changing set of consumers and a universe of situations.

Whatever the challenges of working with teens, a "one-size-fits-all" is destined to fail and generate more costs than benefits. A flexible approach geared to a particular

situation, social networking or other information sharing activity, will clearly provide more benefits than an arbitrary rule that is easy to enforce but with fewer benefits.

Conclusion

The Commission has asked many challenging questions in Appendix A. For many of them it is tempting to follow a knee-jerk response, which would lead to inconsistent and poor choices. We hope that this Comment, showing how the Commission has had experience with these "first principles" in other contexts over the past 40 years, will lead the Commission to a flexible approach to Privacy that will serve well in a quickly changing environment.

We believe that self-regulation is more effective at this point than formal rulemaking. If the Commission opts for some rules, we believe that flexible guides, rather than rigid requirements, would produce more benefits than costs. In short, self-regulation and flexible guides, as in the Red Flags proceeding, is the only way the Commission can nurture a program that can properly be labeled as Privacy by Design.

Sincerely,

Barry J. Cutler
Counsel for ERA

Attachment

APPENDIX A
QUESTIONS FOR COMMENT ON PROPOSED FRAMEWORK

A. Scope

1. Are there practical considerations that support excluding certain types of companies or businesses from the framework — for example, businesses that collect, maintain, or use a limited amount of non-sensitive consumer data?

2. Is it feasible for the framework to apply to data that can be "reasonably linked to a specific consumer, computer, or other device"?

3. How should the framework apply to data that, while not currently considered "linkable," may become so in the future?

4. If it is not feasible for the framework to apply to data that can be "reasonably linked to a specific consumer, computer, or other device," what alternatives exist?

5. Are there reliable methods for determining whether a particular data set is "linkable" or may become "linkable"?

6. What technical measures exist to "anonymize" data and are any industry nouns emerging in this area?

B. Companies should promote consumer privacy throughout their organizations and at every stage of the development of their products and services

Incorporate substantive privacy protections

1. Are there substantive protections, in addition to those set forth in Section V(B)(1) of the report, that companies should provide and how should the costs and benefits of such protections be balanced?

2. Should the concept of "specific business purpose" or "need" be defined further and, if so, how?

3. Is there a way to prescribe a reasonable retention period?

4. Should the retention period depend upon the type or the sensitivity of the data at issue? For example, does the value of information used for behavioral advertising decrease so quickly that retention periods for such data can be quite short?

5. How should the substantive principles set forth in Section V(B)(1) of the report apply to companies with legacy data systems?

6. When it is not feasible to update legacy data systems, what administrative or technical procedures should companies follow to mitigate the risks posed by such systems?

7. Can companies minimize or otherwise modify the data maintained in legacy data systems to protect consumer privacy interests?

C. Maintain comprehensive data management procedures

1. How can the full range of stakeholders be given an incentive to develop and deploy privacy-enhancing technologies?

2. What roles should different industry participants — *e.g.*, browser vendors, website operators, advertising companies — play in addressing privacy concerns with more effective technologies for consumer control?

D. Companies should simplify consumer choice

Commonly accepted practices

1. Is the list of proposed "commonly accepted practices" set forth in Section V(C)(l) of the report too broad or too narrow?

2. Are there practices that should be considered "commonly accepted" in some business contexts but not in others?

3. What types of first-party marketing should be considered "commonly accepted practices"?

4. Even if first-party marketing in general may be a commonly accepted practice, should consumers be given a choice before sensitive data is used for such marketing?

5. Should first-party marketing be limited to the context in which the data is collected from the consumer?

   - For instance, in the online behavioral advertising context, Commission staff has stated that where a website provides recommendations or offers to a consumer based on his or her prior purchases at that website, such practice constitutes first-party marketing. An analogous offline example would include a retailer offering a coupon to a consumer at the cash register based upon the consumer's prior purchases in the store. Is there a distinction, however, if the owner of the website or the offline retailer sends offers to the consumer in another context — for example, via postal mail, email, or text message? Should consumers have an opportunity to decline solicitations delivered through such means, as provided by existing sectoral laws?

6. Should marketing to consumers by commonly-branded affiliates be considered first-party marketing?

7. How should the proposed framework handle the practice of data "enhancement," whereby a company obtains data about its customers from other sources, both online and offline, to enrich its databases? Should companies provide choice about this practice?

E. Practices that require meaningful choice

General

1. What is the most appropriate way to obtain consent for practices that do not fall within the "commonly accepted" category?

2. Should the method of consent be different for different contexts?

   - For example, what are effective ways to seek informed consent in the mobile context, given the multiple parties involved in data collection and the challenges presented by the small screen?

   - Would a uniform icon or graphic for presenting options be feasible and effective in this and other contexts?

   - Is there market research or are there academic studies focusing on the effectiveness of different choice mechanisms in different contexts that could assist FTC staff as it continues to explore this issue?

3. Under what circumstances (if any) is it appropriate to offer choice as a "take it or leave it" proposition, whereby a consumer's use of a website, product, or service constitutes consent to the company's information practices?

4. What types of disclosures and consent mechanisms would be most effective to inform consumers about the trade-offs they make when they share their data in exchange for services?

   - In particular, how should companies communicate the "take it or leave it" nature of a transaction to consumers?

   - Are there any circumstances in which a "take it or leave it" proposition would be inappropriate?

5. How should the scope of sensitive information and sensitive users be defined and what is the most effective means of achieving affirmative consent in these contexts?

6. What additional consumer protection measures, such as enhanced consent or heightened restrictions, are appropriate for the use of deep packet inspection?

7. What (if any) special issues does the collection or the use of information about teens raise?

   - Are teens sensitive users, warranting enhanced consent procedures?

   - Should additional protections be explored in the context of social media services? For example, one social media service has stated that it limits default settings such that teens are not allowed to share certain information with the category "Everyone." What are the benefits and drawbacks of such an approach?

8. What choice mechanisms regarding the collection and use of consumer information should companies that do not directly interact with consumers provide?

9. Is it feasible for data brokers to provide a standardized consumer choice mechanism and what would be the benefits of such a mechanism?

F. <u>Special choice for online behavioral advertising: Do Not Track</u>

1. How should a universal choice mechanism be designed for consumers to control online behavioral advertising?

2. How can such a mechanism be offered to consumers and publicized?

3. How can such a mechanism be designed to be clear, easy-to-find, usable and understandable to consumers?

4. How can such a mechanism be designed so that it is clear to consumers what they are choosing and what the limitations of the choice are?

5. What are the potential costs and benefits of offering a standardized uniform choice mechanism to control online behavioral advertising?

6. How many consumers would likely choose to avoid receiving targeted advertising?

7. How many consumers, on an absolute and percentage basis, have utilized the opt-out tools currently provided?

8. What is the likely impact if large numbers of consumers elect to opt out? How would it affect online publishers and advertisers, and how would it affect consumers?

9. In addition to providing the option to opt out of receiving ads completely, should a universal choice mechanism for online behavioral advertising include an option that

allows consumers more granular control over the types of advertising they want to receive and the type of data they are willing to have collected about them?

10. Should the concept of a universal choice mechanism be extended beyond online behavioral advertising and include, for example, behavioral advertising for mobile applications?

11. If the private sector does not implement an effective uniform choice mechanism voluntarily, should the FTC recommend legislation requiring such a mechanism?

G. Companies should increase the transparency of their data practices

Improved privacy notices

1. What is the feasibility of standardizing the format and terminology for describing data practices across industries, particularly given ongoing changes in technology?

2. How can companies present these notices effectively in the offline world or on mobile and similar devices?

3. Should companies increase their use of machine-readable policies to allow consumers to more easily compare privacy practices across companies?

Reasonable access to consumer data

4. Should companies be able to charge a reasonable cost for certain types of access?

5. Should companies inform consumers of the identity of those with whom the company has shared data about the consumer, as well as the source of the data?

6. Where companies do provide access, how should access apply to information maintained about teens? Should parents be able to access such data?

7. Should access to data differ for consumer-facing and non-consumer-facing entities?

8. For non-consumer-facing companies, how can consumers best discover which entities possess information about them and how to seek access to their data?

9. Is it feasible for industry to develop a standardized means for providing consumer access to data maintained by non-consumer-facing entities?

10. Should consumers receive notice when data about them has been used to deny them benefits? How should such notice be provided? What are the costs and benefits of providing such notice?

Material changes

11. What types of changes do companies make to their policies and practices and what types of changes do they regard as material?

12. What is the appropriate level of transparency and consent for prospective changes to data-handling practices?

H. Consumer education

1. How can individual businesses, industry associations, consumer groups, and government do a better job of informing consumers about privacy?

2. What role should government and industry associations have in educating businesses?