



February 18, 2011

Donald S. Clark
Secretary
Federal Trade Commission
Room H-135 (Annex W)
600 Pennsylvania Avenue, N.W.
Washington, DC 20580

Re: “Protecting Consumer Privacy in an Era of Rapid Change”

Dear Secretary Clark,

The Marketing Research Association (MRA) hereby submits these comments in response to the “Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers” (“the Report”).

TABLE OF CONTENTS

- A. Introduction
- B. Background
- C. Survey and Opinion Research & Privacy
- D. Q&A: Scope
- E. Q&A: Incorporate substantive privacy protections
- F. Q&A: Companies should simplify consumer choice: Commonly accepted practices
- G. Q&A: Practices that require meaningful choice: General
- H. Q&A: Special choice for online behavioral advertising: Do Not Track
- I. Q&A: Companies should increase the transparency of their data practices: Improved privacy notices
- J. Q&A: Companies should increase the transparency of their data practices: Reasonable access to consumer data
- K. Q&A: Companies should increase the transparency of their data practices: Material changes
- L. Conclusion

A. Introduction

MRA respectfully submits these comments in response to the Federal Trade Commission's ("Commission") request for comment to the "Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers" ("the Report"). MRA supports the basic principles of the new framework for consumer privacy proposed in the Report:

- "Privacy by design" – building privacy protections into everyday business practices – is already generally in practice by survey and opinion research profession.
- "Simplified choice" is appealing for both businesses and consumers, although the details of implementation matter greatly. MRA believes in a use-based approach, where the reason behind data collection, use and sharing is more important than the specific kind or type of data. The Commission's proposal to make privacy choices uniform and comprehensive sounds appealing, but, certainly as it pertains to data used for survey and opinion research, one size will definitely not fit all.
- Transparency in data practices is a laudable goal, one which the research profession is working towards, but the principle of "access" to data does not properly apply to research, as we will discuss.
- Consumer education has been an ongoing challenge for the research profession, and one that MRA has tried to tackle with various initiatives, such as the "Your Opinion Counts" program.

Regulatory approaches that balance privacy with the free flow of information are extremely important to the research profession, and MRA is concerned that the Commission may be pursuing broad privacy initiatives without fully weighing potential costs and benefits to businesses and consumers and without specifically identifying harms in need of redress.

These comments will assess the current self-regulatory framework for privacy in the survey and opinion research profession and offer some answers to the inquiries raised in the Report by the Commission.

B. Background

MRA, a non-profit national membership association, is the leading and largest association of the survey and opinion research profession. MRA promotes, advocates and protects the integrity of the research profession and strives to improve research participation and quality.

The research profession is a multi-billion dollar driver of the worldwide economy, comprised of pollsters and government, public opinion, academic and goods and services researchers, whose companies and organizations range from large multinational

corporations to small or even one-person businesses. In fact, U.S. government entities like the Commission are, as a group, the single largest purchaser/user of research from the survey and opinion research profession.

Survey and opinion research is the scientific process of gathering, measuring and analyzing public opinion and behavior. On behalf of their clients -- including the government (the world's largest purchaser), media, political campaigns, and commercial and non-profit entities -- researchers design studies and collect and analyze data from small but statistically-balanced samples of the public.¹ Researchers seek to determine the public's opinion regarding products, services, issues, candidates and other topics. Such information is used to develop new products, improve services, and inform policy.

C. Survey and Opinion Research & Privacy

Research data is not normally reported by individual answers. Instead, each person's responses are aggregated with many others and then reported as a group. Moreover, most research companies destroy individual data records at the end of the study, and names and contact information of participants are separated from the answers if additional tabulation of the results is conducted. Again, all of the personally identifiable records are usually destroyed after the study is completed or the validation check has been made, and all of a respondent's personally identifiable information is kept strictly confidential. Legitimate survey and opinion researchers do not divulge the identity, personal information or individual answers of a research participant unless granted permission to do so by the participant.

Due to the nature of the survey and opinion research process, confidentiality is the bedrock of the research process and the resultant industry codes and guidelines, like the MRA Code of Marketing Research Standards.² Members of MRA are bound by their ethical obligation to protect the privacy and confidentiality of research participants and their data and obtain consent prior to sharing any personally identifiable information. MRA's members work to uphold the Federal Trade Commission's Fair Information Practice Principles and best practices on the handling of personal information.

Survey and opinion research is thus sharply distinguished from commercial activities, like marketing, advertising and sales. In fact, MRA and other research associations prohibit sales or fundraising under the guise of research (referred to as "sugging" and "frugging") and any attempts to influence or alter the attitudes or behavior of research participants as a part of the research process. Research can never be connected to a sales or marketing pitch. Quite to the contrary, professional research has as its mission the true and accurate assessment of public sentiment in order to help individuals, companies and organizations design products, services and policies that meet the needs of and appeal to the public.

¹ A "sample" is a subset of a population from which data is collected to be used in estimating parameters of the total population.

² <http://www.mra-net.org/resources/documents/CodeMRStandards.pdf>

D. Q&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?”

MRA asserts that survey and opinion research should be affirmatively excluded from many aspects of the Report’s privacy framework. Survey and opinion research is an inherently non-commercial activity and thus outside the realm of what FTC Chairman Jon Leibowitz called “the commercial world” in his remarks.³ The Report asserts that, “the framework would apply to all commercial entities that collect consumer data in both offline and online contexts, regardless of whether such entities interact directly with consumers”. While for-profit survey and opinion research businesses may well be deemed to be commercial entities, the collection and use of data for research purposes is non-commercial. Therefore, research purposes should be excluded.

2) “Is it feasible for the framework to apply to data that can be “reasonably linked to a specific consumer, computer, or other device”? How should the framework apply to data that, while not currently considered “linkable,” may become so in the future? 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?”

The common standard in U.S. laws is personally identifiable information (“PII”) (first name and last name with contact or location information) combined with social security numbers, or financial account or credit information, that could allow for identity theft, fraud or other kinds of direct consumer harm. Other information, or combinations of information, can float publicly (or not), but are not broadly recognized as posing a threat of harm. It is very difficult to go beyond that standard without sliding down a slippery slope where most every piece of information could be considered “linkable” and thus restricted.

E. Q&A: 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?

The Report lays out four substantive protections that companies should provide:

³ “Remarks of Chairman Jon Leibowitz Prepared for Delivery”, Dec. 1, 2010.
<http://www.ftc.gov/speeches/leibowitz/101201privacyreportremarks.pdf>

- “reasonable safeguards” to protect data, with the “level of security required” depending “on the sensitivity of the data, the size and nature of a company’s business operations, and the types of risks a company faces”;
- collecting “only the information needed to fulfill a specific, legitimate business need”, also known as data minimization;
- “reasonable and appropriate data retention periods, retaining consumer data for only as long as they have a specific and legitimate business need to do so”; and
- “reasonable steps to ensure the accuracy of the data they collect, particularly if such data could be used to deny consumers benefits or cause significant harm.”

The first two protections are appropriate and relatively universal.

Data retention periods could be problematic, should the Commission decide to determine the length of those periods itself. Specifically, within various modes and methods of survey and opinion research, the need to retain data will vary, and should be properly subject to those needs, not an arbitrary decision by a regulatory body unfamiliar with the processes and practices of research. Additionally, a major objective of research is to understand attitudes, behaviors and opinions over-time. The collection and analysis of this information often leads to new theories over time, requiring the re-visiting of older data. Because of this, prescribed retention periods would diminish the long-term value of data collected for research purposes. The Commission should avoid setting time constraints without being familiar with the processes and practices of all businesses that would be impacted by their implementation, including the many processes and practices of survey and opinion research.

Accuracy is certainly of prime concern to research businesses. The biggest debates within the survey and opinion research profession over the last few years have revolved around the improvement of data quality and concerns about fraudulent or inaccurate data coming from some research participants. The profession has worked on numerous approaches to deal with such problems, such as better authentication of participants and further education of consumers as to the value of research and the need for honest participation. MRA would, however, be wary of regulatory requirements for “accuracy” since the “harms” conceived of by the Commission, such as credit penalties or reputation impact, should never result from the use of data for research purposes.

2) Is there a way to prescribe a reasonable retention period? 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?

MRA remains opposed to a definitive “reasonable retention period”, since what might suit commercial or advertising purposes would have no relation to the many and varied forms of survey and opinion research.

F. Q&A: Companies should simplify consumer choice: Commonly accepted practices

1) Is the list of proposed “commonly accepted practices” set forth in Section V(C)(1) of the report too broad or too narrow? Are there practices that should be considered “commonly accepted” in some business contexts but not in others?

The Reports lists the following as “commonly accepted practices for which companies should not be required to seek consent once the consumer elects to use the product or service in question”: product and service fulfillment, internal operations (including customer satisfaction research), fraud prevention, legal compliance and public purpose, and first-party marketing.

Aside from customer satisfaction research, survey and opinion research does not fit into any of the buckets above. That is mostly because the Commission has not noticeably considered how the proposals contained in the Report would impact research. Although research is not easily simplified into something like a “commonly accepted practice”, perhaps it should be.

The Commission frequently uses survey and opinion research – it would appear that the Commission already treats research as a “commonly accepted practice.”⁴ There remains a need to exempt survey and opinion research from most requirements and restrictions envisioned by this Report.

G. Q&A: Practices that require meaningful choice: General

1) 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?

This is one of the most contentious areas in any data privacy debate because the definition of “sensitive” is ultimately in the eye of the beholder. The Report heightens the tension by proposing that collection, use or sharing of sensitive information would require prior “affirmative express consent”.

The Report does not define what “sensitive” information is, although it would appear to at least include, “information about children, financial and medical information, and precise geolocation data.” Information garnered via “deep packet inspection” would also be subject to the “sensitive” treatment.

The Report’s approach to so-called “sensitive” information presents several problems.

⁴ For instance, see Page 61 of the Report: “Market research and academic studies focusing on the effectiveness of different choice mechanisms in different contexts would be particularly helpful to staff as it continues to explore this issue.” Also, on Page 71 of the Report, the FTC cites how “eight agencies worked together to develop a model financial privacy notice using extensive research and consumer testing” – a great example of survey and opinion research in action.

First, while MRA understands the concern for privacy of bona fide medical records, the definition of “medical information” could be construed to mean far more than actual records of a doctor or hospital (such as one would consider to be protected health information under HIPAA). If a telephone survey were to ask a research participant, “Have you ever suffered from one of the following illnesses”, would the resulting data constitute medical information according to the Commission? How about responses to a question such as, “How are you feeling today? Are you feeling better or worse than yesterday?” Such questions are quite common in research studies and would seem to run afoul of the Report’s restrictions on sensitive information.

Second, clarification on the definition of “financial information” would be necessary to ensure that it does not include data on a research participant’s individual or household income – one of the most common categories of demographic data in any research study.

Third, the use of the term “geolocation” or other geospatial relevant terminology could severely impact survey and opinion research, especially absent careful and limited definition. Does the term refer to the actual location of an individual at any given time, such as the location information provided by cell phone triangulation or GPS? Or does it mean an actual street/house address (something which is commonly available in phone books and public records and essential to constructing representative samples of the population using statistical weighting and stratification).

Fourth, the Report fails to limit the definition of “sensitive” information. Will it be expanded to include even more demographic data common or important to survey and opinion research, like race, ethnicity, sexual orientation or behavior, and religious affiliation?⁵

Finally, the Report appears to treat certain kinds of information, on their own, as “sensitive”, instead of requiring such information to be connected with data that is personally identifiable.

2) What (if any) special issues does the collection or the use of information about teens raise? Are teens sensitive users, warranting enhanced consent procedures?

While MRA does recommend that survey and opinion researchers treat collection, use and sharing of data from any research participant under the age of majority in a more careful fashion, including seeking parental consent such as may be feasible or practical in the research process, MRA resolutely opposes: (1) raising the age limit on the Children’s Online Privacy and Protection Act (COPPA), for instance, beyond the existing restrictions on children under 13 years of age; and (2) applying COPPA-style restrictions to offline data. Enhanced protections can be encouraged by self-regulatory bodies, while leaving research companies the flexibility to determine how best to implement such protections and in what context.

⁵ That was certainly the case with Rep. Rush’s “Best Practices Act” (H.R. 5777).

3) Should additional protections be explored in the context of social media services?

While MRA does not support additional legal protections at this time over the continually evolving social media sphere, we have been working with our members and the broader survey and opinion research profession to grapple with the difficult questions raised by research in the social space or using social media data. Most recently, MRA released a “Guide to the Top 16 Social Media Research Questions”,⁶ raising important ethical concerns, such as:

- Question # 7: “Are the participants aware that their user-generated content is under observation?”
- Question # 9: “What are the controversies and legal issues regarding the rights of the people whose data is being used?”
 - This question delves into concerns over privacy, the interaction with individuals, and “Combining data from multiple sources where privacy policies differ”.

Legislation and regulation are always in danger of being obsolete before they are even finalized – this is even more so the case when dealing with social media, where networks, trends, styles, and websites, rise, change, and fail, every day.

4) What choice mechanisms regarding the collection and use of consumer information should companies that do not directly interact with consumers provide? Is it feasible for data brokers to provide a standardized consumer choice mechanism and what would be the benefits of such a mechanism?

There are plenty of companies and organizations that may not directly interact with consumers, but are part of the research chain and handle consumer’s data as part of that process. While this could include somewhat mundane parts of the chain, such as companies that translate or otherwise process survey data, companies that provide research samples would be most prone to this mis-placed concern. Although sample providers superficially appear to fit into the same category as a data broker, their business is in fact quite different. A sample provider does not buy and sell information for various purposes to and from various entities – it buys and sells information on groups of research subjects strictly for the purpose of informing particular research questions and studies.

H. Q&A: Special choice for online behavioral advertising: Do Not Track

1) How should a universal choice mechanism be designed for consumers to control online behavioral advertising? How can such a mechanism be offered to consumers and publicized? How can such a mechanism be designed to be clear, easy-to-find, usable, and understandable to consumers? How can such a mechanism be designed so that it is clear to consumers what they are choosing and what the limitations of

⁶ http://www.mra-net.org/rq/MRA_IMRO_SMR16.cfm

the choice are? What are the potential costs and benefits of offering a standardized uniform choice mechanism to control online behavioral advertising? How many consumers would likely choose to avoid receiving targeted advertising? How many consumers, on an absolute and percentage basis, have utilized the opt-out tools currently provided? 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? 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? Should the concept of a universal choice mechanism be extended beyond online behavioral advertising and include, for example, behavioral advertising for mobile applications? If the private sector does not implement an effective uniform choice mechanism voluntarily, should the FTC recommend legislation requiring such a mechanism?

The privacy innovation demonstrated by the advertising industry's new dynamic web icons and the development of do-not-track options built into new versions of Microsoft's Internet Explorer, Mozilla's Firefox and Google's Chrome web browsers could only emanate from the free market. It is a privacy model that revolves around the consumer and the marketplace, not government fiat.

The Report does reference these options, but worries that consumers "may be confused" or "may believe" or "are not likely to be aware". This section of the Report promotes a "Do Not Track" mechanism. However, the Commission has not given these various private-sector initiatives any time to see if they actually work, if consumers like or want them, and certainly if consumers are "confused" or even "aware" of what they are, how they operate, and the consequences of using them. More importantly, although the Commission identifies hypothetical consumer "confusion" and a lack of awareness, why not consider some further consumer education?

As it pertains specifically to research, MRA is concerned that, though the Commission addresses their concerns by referencing "online behavioral advertising", the use of behavioral tracking for research purposes could inadvertently be constrained as well. This could strangle many possible new methods of research – methods that could better serve consumer choice and privacy than current methods – before they've even been conceived. Such research could have profoundly positive benefits for consumers and such public good is worth preserving.

MRA would like to see an approach to online tracking that differentiates by the purpose and use of the data collected – in particular, that differentiates research purposes from commercial/advertising purposes. While online behavioral tracking may be conducted by research firms and organizations, it would be for aggregating groups and segments of the online population, not targeting specific individuals for sales or advertising.

Given that the Commission refers to a “Do Not Track” mechanism for handling online tracking, such a distinction is all the more relevant. The distinction between marketing calls and non-commercial calls are the cornerstone of the extremely popular Do Not Call Registry, which shields consumers who so request shielding from unrequested telemarketing telephone calls, while allowing calls for survey and opinion research purposes.

I. Q&A: 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?

The Report asserts that, “Companies should standardize the format of their notices, as well as the terminology used.” While it might be possible to standardize the format and terminology for describing data practices within certain industries, doing so across industries could prove very difficult. MRA does not know whose standard could ever cover both the myriad of commercial enterprises and survey and opinion research.

The purpose and data practices of the research profession differ significantly from most commercial enterprises. More importantly, as a vibrant and evolving profession, data practices within research are difficult to standardize because modes and methods differ dramatically across the profession. This is partially because of advances in technology, but more because of advances and refinements in social science.

MRA already requires that researchers seek transparency with regard to clients, research participants, and the public at large⁷ while trying not to micromanage that transparency, given that different modes and methods of research will require tailor-made approaches.

J. Q&A: Companies should increase the transparency of their data practices: Reasonable access to consumer data

Access to consumer data may make sense in contexts where such data (particularly if inaccurate) could adversely impact a consumer’s credit rating, personal or professional

⁷ For instance, in the MRA Code, Part A of the Preface describes the purpose of code in providing fairness, confidence in research, and ethics towards research participants. In the Code itself, item 3 requires disclosures for public-release research; item 7 requires that research be reported accurately and honestly; item 12 forbids researchers from misrepresenting their qualifications and experience; item 21 forbids representing a non-research activity to be research; item 25 requires that research participants are informed at the outset if interviews/discussions are audio/video recorded; item 31 demands that researchers make factually correct statements, whether verbal or written, to secure cooperation and honor promises made during the interview to research participants; item 54 requires researchers to provide access to their privacy policies; and item 55 obliges researchers to provide participants the choice with each survey to be removed (opt-out) from future Internet invitations.

reputation, or likelihood of becoming a victim of identity theft. None of these conditions should reasonably be assumed to apply to survey and opinion research data.

Participation in survey and opinion research is voluntary. Research best practices already require disclosure of what data is being collected and used, and for what purpose, and that participants be given the opportunity to opt out.

The “cost of access to businesses” and “the ability of companies to authenticate the identity of consumers requesting access” are indeed serious concerns and weigh heavily against survey and opinion research companies being required to grant access. Since the research process is interested in broad groups, not individuals, compiling and tracking individual consumer data would require complex and expensive procedures and infrastructure not currently in use. Moreover, such tracking could lead to a much greater threat of harm from data leakage – and empower the kind of consumer tracking that the FTC seems to fear.

MRA supports the concept of a “sliding scale” for access in order to reconcile the vague benefits with the expected costs. We propose that the availability and extent of access should depend on the data actually being capable of being used for identity theft and/or actually sensitive as we discussed earlier. More importantly, the use of the data should matter, and survey and opinion research data should, in most cases, not be subject to access – especially given that consumer concern focuses on commercial data brokerage for marketing and credit purposes, not on research.

2) Should access to data differ for consumer-facing and non-consumer-facing entities? For non-consumer-facing companies, how can consumers best discover which entities possess information about them and how to seek access to their data? Is it feasible for industry to develop a standardized means for providing consumer access to data maintained by non-consumer-facing entities?

As mentioned previously, research companies that are not consumer-facing are only dealing with participants’ data for strictly research purposes – as such, they should be on the research end of any sliding scale, and excluded from most worries about access. If access were to be deemed necessary to be provided by such companies, the specifics of implementation would need to be determined on an industry-by-industry basis.

K. Q&A: Companies should increase the transparency of their data practices: Material changes

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

Providing notice (and securing some form of retroactive consent) for material changes to privacy practices/policies is now standard. MRA considers notice with an opt-out to be a reasonable expectation, but opposes an express affirmative consent standard.

Such a standard is ill-suited to research, and would be most debilitating for online panel companies and online research communities (who keep huge rosters of participants) and focus group facilities (who maintain large lists of potential participants). It would likely be impossible to get express affirmative consent from millions of people before changing a policy or practice.

L. Conclusion

Survey and opinion researchers already encounter significant public apathy with respect to research participation. Research “response” rates have been falling for the last couple of decades, driving up the cost of and time involved in achieving the required number and strata of participants to reach viable representative samples for most research studies. That is part of what informs MRA’s concerns with the Report: that the challenges identified above will make it harder to reach and involve research participants, increase non-response bias and adversely impact the accuracy of research results.

This wouldn’t just impede bona fide survey and opinion research. It would ultimately result in higher costs for research – costs which would be passed on to the individuals the Commission is trying to protect, in the form of:

- higher prices for goods and services;
- lengthier time before new or better goods and services are brought to the marketplace;
- delayed introduction of new or better public policies; and
- a decreased amount of research ordered by companies, who might then bring less well-tested and researched products and services to market, harming consumers in the end because the goods and services did not fulfill consumer expectations or needs.

Moreover, while the Commission has no jurisdiction over not-for-profits and governmental entities, every link in the research chain would be impacted by the Report’s proposals and imperil their research – and goals – in turn.⁸ These challenges would ultimately pose a threat to the American economy, with domestic companies weakened in the global marketplace by attempts to use intuition and guess-work in place of tested research methods.

MRA first and foremost requests that the Commission support a truly self-regulatory approach to data privacy. Non-governmental entities, particularly trade and professional associations, are in a superior position to agree upon and enforce privacy principles in the private sector.

⁸ The proposed restrictions and changes in the Report could severely hinder government research, including the Commission’s own. They would certainly restrict research sponsored by government, just like research sponsored by anyone else. Moreover, agencies like the National Center for Healthcare Statistics (NCHS), which do most of their research in-house, must still rely on private for-profit sampling companies for their participant contact lists.

As regards the survey and opinion research profession, leading research practices widely adopted by members of various research associations are the best way to produce effective research while safeguarding research participants' privacy. In addition to the many best practice guidelines promulgated by MRA, effective self-regulation can be seen in the codes and standards of MRA and other research associations. As well, long-standing privacy seal programs like TRUSTe and BBBOnline, and the innovative privacy icons developed by advertising groups, demonstrate a keen commitment to transparency and consumer choice in the private sector.

Unlike government legislation and regulation, professional codes and standards are developed by the practitioners themselves, flexible in the face of technological and business innovation, and easier to improve and perfect over time.

MRA also requests that bona fide survey and opinion research, as we have defined it earlier, be explicitly excluded from a majority of the proposals in this Report and that the Commission focus efforts on strictly commercial data practices.

MRA and the whole survey and opinion research profession stand ready to work with you in pursuit of these goals. For the reasons illuminated in this comment, MRA respectfully requests the Commission to re-examine the privacy principles proposed in the Report.

Sincerely,



Howard Fienberg, PLC
Director of Government Affairs
Marketing Research Association
Howard.Fienberg@mra-net.org
1111 16th St. NW, Suite 120
Washington, DC 20036
Phone: (202) 775-5170
Fax: (888) 512-1050
Email: howard.fienberg@mra-net.org
<http://www.mra-net.org>