



Marketing Research Association

Marketing Research Association, Inc.

THE CODE OF MARKETING RESEARCH STANDARDS

Ratified March, 2007

INDEX

PREFACE	PAGE
A. Purpose of the Code of Marketing Research Standards	3
B. Background of the Code of Marketing Research Standards	3
C. Using This Document	3
D. Definitions	4
MRA CODE OF MARKETING RESEARCH STANDARDS	5
(with explanatory notes)	
Sampling	12
Tabulation and Data Processing	14
APPENDIX	15
A. Enforcement and Filing a Complaint	16
B. How to Comply With The Children's Online Privacy Protection Rule	19
C. Compliance with Government Legislation	24
D. IMRO Standards with full detail Position Papers	26
E. Mystery Shopping	30
F. Sales Waves	31
G. Auto-Dialing Systems with CATI	32
H. Transaction-based Customer Satisfaction Confidentiality	35

PREFACE

A. Purpose of the Code of Marketing Research Standards

The Marketing Research Association's Code of Marketing Research Standards is established to ensure that MRA members conform to the following principles:

- ▶ Conduct research in an honest and ethical manner
- ▶ Instill confidence in research to encourage public cooperation
- ▶ Instill confidence that research is done in a professional and fair manner
- ▶ To provide members with guidelines that lead to research being conducted in accordance with scientific, statistical and proven practical methods.
- ▶ Carry out every research project in accordance with the Code
- ▶ Respect the general public and its rights

The principles of this Code must be adhered to and signed by each member of the Marketing Research Association, both corporate and individual, **as a condition of membership in MRA**.

Nonmembers of MRA are encouraged to familiarize themselves with this Code to facilitate their dealing with MRA members and to use as an educational tool.

B. Background of the Code of Marketing Research Standards

The Marketing Research Association is a recognized leader in the opinion and marketing research industry, advancing practical application, use and understanding of the opinion and marketing research profession.

A fundamental aim of the Association is to ensure that standards are maintained. It is important that opinion and marketing research knowledge and the value of research are communicated to both the business community and the public at large, while complying with applicable federal, state and local laws, regulations and ordinances.

MRA expects members to follow principles of honesty, professionalism, fairness and confidentiality to guard the interests of the public and our clients in order to promote good business practices. MRA's Code of Marketing Research Standards addresses the responsibilities of our members, not only to each other, but also to the general public and business community.

Researchers must not, whether knowingly or negligently, act in any way that could bring discredit to, or compromise public confidence in, the marketing research profession.

All MRA members must sign the Endorsement Agreement that accompanies the Code as a condition of membership. The agreement lays out the basic principles that members agree to abide by (honesty, integrity, respect for the public, professionalism and fairness, and commitment to the Code). Failure to sign the agreement will bar the company or individual from MRA membership.

C. Using This Document

The Code of Marketing Research Standards is structured to include those standards by which ethical researchers must abide. As MRA is an Association that serves all segments of the profession, its Code encompasses standards for End Users/Research Buyers, Research Providers/Suppliers/ Data Collectors and Related Service Providers. Certain Related Services are considered so specialized as to warrant their own set of standards. These segments are Sampling and Tabulation & Data Processing.

MRA offers "Recommended Best Business Practices" as a separate document. MRA presents those recommended best business practices as ideals to guide Opinion and Marketing Researchers in providing professional, ethical and reliable products and services. Recommended Best Business Practices is to be used as a supplement to the enforceable Code of Marketing Research Standards.

DEFINITIONS

As referred to in this document, the following definitions apply:

Client: The entity or entities who has/have engaged the performance of services.

Conflict of Interest: Any situation in which an individual or corporation is in a position to exploit a professional or official capacity in some way for their personal or corporate benefit.

Data: A group of facts or statistics. A plural noun.

Data Collection: Those individuals and companies engaged in the gathering of data from a primary source. Those engaged in this segment of the profession are usually the direct line of communication with the general public and businesses via e-mail, telephone, face-to-face or mail interviews.

End User: The ultimate recipient and user of the results of the data gathered and analyzed. Also called a “Research Buyer”.

Push Poll: A telemarketing technique in which telephone calls are used to canvass potential voters, feeding them false or misleading ‘information’ about a candidate under the pretense of taking a poll to see how this ‘information’ affects voter preferences. In fact, the intent is not to measure public opinion but to manipulate it-to ‘push’ voters away from one candidate and toward the opposing candidate. Such polls defame selected candidates by spreading false or misleading information about them. The intent is to disseminate campaign propaganda under the guise of conducting a legitimate public opinion poll.

Qualitative Research: Research conducted to find in-depth information about a subject or issue. It is an open-ended method of acquiring information not subject to quantitative or mathematical methods of analysis. Qualitative researchers use subjective means to evaluate information.

Quantitative Research: Research conducted to obtain statistically reliable and projectable numerical data. Quantitative researchers use objective means to evaluate information via mathematical methods of analysis.

Research Design and Analysis: That segment of the research process that is responsible for defining the research problem, planning the study design, crafting of questionnaires and analyzing and presenting the data. Those engaged in this segment of the profession usually interact directly with the End User. Sometimes referred to as Research Providers or Research Suppliers.

Sample: Verb: The statistical selection of some respondents to represent the opinions of many. Noun: A usable dataset comprised of a population subset selected for use in a specific research project.

Sample Provider: A company that supplies sample for use in marketing research projects. This can be a company whose exclusive business is providing sample or it can be any other entity in the research process that provides sample for the use of data collection, e.g. End User-provided sample.

Simulated Test Market: A quantitative procedure designed to create conditions that approximate the actual marketplace in order to determine a product’s potential sales and/or market share. This staged advertising and purchase process often employs a mock-up of store shelves containing relevant product at which a respondent may “shop” for product by browsing through the “store”.

Tabulation and Data Processing: Those individuals and companies engaged in the computation of data in order to generate a desired outcome. Encompasses the functions of receiving, entering, sorting, abstracting, distributing and storing of data.

MRA CODE OF MARKETING RESEARCH STANDARDS

Explanatory notes (*italics*) are provided to clarify, elucidate or illustrate but do not in any way limit the application or interpretation of the Code.

SECTION A:

All Marketing Research Association Members agree that they:

1. Will ensure that each study is conducted according to the agreement with the Client.

Procedures should be implemented to confirm or verify that client specifications are being followed.

2. Will never falsify or omit data for any reason at any phase of a research study or project.

It is a basic tenet of the profession, and incumbent on every MRA member to conduct the business of survey and opinion research with the utmost of integrity. Falsifying data of any kind for any reason, or omitting data that do not conform to preconceived notions, will not be tolerated.

3. All marketing and opinion research released for public consumption (e.g. p-r release research) will comply with prevailing research standards specified in this Code and include statements disclosing (1) the method of data collection, (2) the date(s) of data collection, (3) the sampling frame, (4) the sampling method, (5) the sample size, and (6) the calculated margin of error for quantitative studies.

Public “Release research (p-r research) is research conducted for the purpose of generating media-worthy headlines. This research can be conducted solely for this purpose or can be comprised of results extracted from research whose objectives were broader but whose outcomes lend themselves to release to the media. The overriding ethos regardless of the intended use of the research is to produce accurate statistics that have significance.

4. Will protect and preserve the confidentiality of all research techniques and/or methodologies and of information considered confidential or proprietary.

Many end-users and research firms have developed research procedures and methodologies that they consider proprietary, including survey techniques, the manner in which questionnaires and questions are constructed, and particular statistical procedures. Members are expected to take all reasonable care in maintaining the confidentiality of these methods and procedures.

5. Information will not be revealed that could be used to identify respondents without proper authorization.

In order to obtain unbiased information during the data collection process, it is often required that the name of the client not be revealed to the respondent during data collection. Members are expected to observe this operational requirement. If the respondent demands to know the name of the sponsor of the research project, that name can only be revealed with the client’s permission and only after the respondent has completed the data collection phase of the research.

6. Will observe confidentiality with all research techniques or methodologies and with information considered confidential or proprietary. Information will not be revealed that could be used to identify clients or respondents without proper authorization, the exceptions being:

- ▶ Customer Satisfaction Research where the express, expected result of all parties is that the client or client’s agent will receive the information for follow-up.
- ▶ Compliance with a court order or other legal demand (e.g. discovery phase of a pending legal case).

Other than the exceptions noted, respondent information will be linked to data collected for research purposes only and will not be used for any purpose other than legitimate research. Members must

protect the confidentiality of anything learned about the respondent.

7. Will report research results accurately and honestly.

Describe how the research was done in enough detail that a skilled researcher could repeat the study; provide data representative of a defined population or activity and enough data to yield projectable results; present the results understandably and fairly, including any results that may seem contradictory or unfavorable.

8. Will protect the rights and privacy of respondents.

Respondent cooperation is dependent upon their expectations that their privacy will not be violated. All reasonable care must be taken to safeguard all respondent information and to ensure that it will be used only as necessary and for legitimate research purposes only.

9. Will treat respondents in a professional manner.

Those engaged in any phase of the research process will maintain high standards of personal conduct in their interaction with respondents

10. Will take all reasonable precautions that respondents are in no way directly harmed or adversely affected as a result of their participation in a marketing research project.

All products will be fit and safe for use. All personally identifiable information will be kept confidential. The facilities in which personal interviews take place will provide a safe atmosphere.

11. Will not abuse public confidence in opinion and marketing research.

Marketing research shall be conducted and reported for the sole purpose of providing factual information.. At no time is marketing research information to be used to intentionally mislead public opinion. Instances of abuse of public confidence undermine the credibility of our profession.

12. Will not misrepresent themselves as having qualifications, experience, skills, resources or other facility locations that they do not possess.

Research professionals should not imply to clients and prospective clients that they possess, own or manage specific capabilities in-house if they do not; ; research professionals may claim only legitimate academic degree(s), clients and professional qualifications and experiences.

13. Will not refer to membership in the Marketing Research Association as proof of competence.

While members can state their membership in the Association, they cannot claim that this automatically conveys a message of their competency to carry out the marketing research process. As members in good standing they can state that they have signed and adhere to the Code

14. Will not ask our members who subcontract research to engage in any activity that is not acceptable as defined in the Code or that is prohibited under any applicable federal, state or local laws, regulations and/or ordinances.

All MRA Members have agreed to comply with the Code as written and thus will not agree to, or ask anyone else to, knowingly violate any of the points of the Code.

15. Will protect the confidentiality of anything learned about a client's business as a result of access to proprietary information

Protecting the confidentiality of a client's business, and the type of research they are conducting, are of paramount importance. Any proprietary information learned about a client's business will not be divulged to a third party without the express written consent of the client..

16. Will, when conducting secondary research, make the End User aware of the source of the secondary research. At no time will secondary research be presented to the End User as primary data.

Misrepresenting data sources can skew interpretation of said data and lead to false or misleading conclusions.

17. Will inform the client if:

- ▶ their work is to be combined or syndicated with other clients' work
- ▶ all or part of their work will be subcontracted outside the researcher's organization

Clients must receive wholly those services and results for which they have paid.

18. Will avoid all conflicts of interest in the carrying out of work for multiple clients, particularly those in the same or similar businesses.

Clients must be assured that any work produced and any findings resulting from that work are their property exclusively. There can be no overlap in the recruiting of respondents, no multiple interviews, and no migration of data from one client's business to another's.

19. When having responsibility for creating products and services for respondent use, will be responsible for providing products and services that :

- ▶ are safe and fit for their intended use
- ▶ are labeled in accordance with all laws and regulations
- ▶ will provide means to make the respondent whole should problems arise
- ▶ will provide emergency contact information

End User will ensure that all test products are in compliance with all safety standards and that all product contents information is provided to the appropriate researchers in the study chain. Data Collectors should request in writing all pertinent information as well as emergency numbers for respondents and themselves.

20. Will provide detailed written or verbal study instructions to those engaged in the data collection process.

To ensure the success of the research, detailed instructions are to be provided prior to the start of any project. These instructions must be confirmed for understanding, ability of the agency to implement and agreement to comply.

21. Will not represent a non-research activity to be opinion and marketing research, such as, but not limited to:

- ▶ questions whose sole objective is to obtain personal information about respondents whether for legal, political, commercial, private or other purposes
- ▶ the compilation of lists, registers or databanks of names and addresses for any non-research purposes (e.g. canvassing or fund raising)
- ▶ industrial, commercial or any other form of espionage that could cause harm to an individual or organization
- ▶ the acquisition of information for use by credit rating services or similar organizations
- ▶ sales or promotional approaches to the respondent
- ▶ the collection of debts

This does not refer to simulated test market research projects when no money is involved or when the money is returned to the respondent at the end of the study. Nor does it refer to Customer Satisfaction Research where the express, expected result of all parties is that the client or client's agent will receive the information for follow-up.

Refer to Appendix E for further details on simulated test market research projects.

22. Will identify surveys and other methods of data collection as such and not attempt to collect data through casual or conversational means other than for bona fide mystery shopping assignments.

Respondents must be aware that the information and/or opinions they are giving will be utilized in some way as survey data, whether qualitative or quantitative. Exception is made for Mystery Shopping as discussed and defined in Appendix E of this Code.

23. Will not use research information to identify respondents without the permission of the respondent. The following are exceptions:

- ▶ Respondent identification information may be used in processing the data and merging data files.
- ▶ Respondent identification information may be used to append client or third-party data to a survey-based data file.
- ▶ Respondent identification information may be revealed in compliance with a court order or other legal demand from a competent and recognized legal authority (e.g. discovery phase of a pending legal case).
- ▶ If such permission is given, the interviewer must record it, or a respondent must do so during all surveys not involving an interviewer, at the time the permission is secured. If such permission is given, the data may only be used for the purpose to which the respondent agreed.

Additionally, members will ensure that all respondent identification information is safeguarded against unauthorized access.

Respondent information will be linked to data collected only for research purposes such as validation, merging survey data with client and third-party data bases, evaluating data in aggregate based on demographic information, and modeling. Providing respondent information is not permissible for any purpose other than legitimate research purposes. If a client requests respondent-identifiable information it will be provided only upon receipt of written declaration of and agreement to a specific intended use. The validity of such use will be determined by the holder of the data and must qualify as a legitimate research use (i.e. validation, planned recalls, modeling, demographic analysis). No other use of this information is allowed within the boundaries of the Code. This applies to all types of respondent sample sources including client-supplied lists. Respondents will be assured that personally identifiable information will remain confidential and be used for research purposes only.

24. Will respect the respondent's right to withdraw or to refuse to cooperate at any stage of the study and will not use any procedure or technique to coerce or imply that cooperation is obligatory.

Respondent cooperation is strictly on a voluntary basis. Respondents are entitled to withdraw from an interview at any stage or to refuse to cooperate in a research project. Interviewers should never lead respondents to believe they have no choice in their participation.

25. Will ensure that respondents are informed at the outset if the interview/discussion is being audio or video recorded by any means and will, if required, obtain written consent if the recorded interview/discussion will be

- ▶ viewed by a third party
- ▶ reproduced for outside use

Sound business practice dictates obtaining the respondent's consent for a defined specific use of his/her voice or image. When using electronic recording equipment, all applicable state and federal laws must be followed.

26. Will give respondents the opportunity to refuse to participate in the research when there

is a possibility they may be identifiable even without the use of their name or address (e.g. because of the size of the population being sampled).

Respondent cooperation is strictly on a voluntary basis. Respondents are entitled to withdraw from a research project. Company policies and/or interviewer instructions should state that the interviewer must give respondents the opportunity not to participate for any reason.

27. Will adhere to the Children's Online Privacy Protection Act and will obtain permission and document consent of a parent, legal guardian or responsible guardian before interviewing children under 13 years of age. Prior to obtaining permission, the interviewer should divulge the subject matter, length of the interview and other special tasks that may be required of the respondent.

Interviewers must take special care when interviewing children or young people. The informed consent of the parent or responsible adult first must be obtained for interviews with children. Parents or responsible adults must be told some specifics about the interview process and special tasks, such as audio, video or IVR recording, taste testing, respondent fees before permission is obtained. All researchers must adhere to all federal and state regulations regarding the interviewing of children under 13 years of age. All interviews conducted online must adhere to the Children's Online Privacy Protection Act (COPPA). Refer to Appendix D of this document for more details on COPPA.

Full text of COPPA available at the following FTC site locations:

*<http://www.ftc.gov/bcp/conline/edcams/kidzprivacy/biz.htm>, <http://www.ftc.gov/privacy/coppafaqs.htm> ,
http://www.ftc.gov/bcp/conline/edcams/kidzprivacy/files/coppa-full_files/frame.htm .*

28. Will ensure that the results of the research are the sole property of the End User(s). At no time will results be shared with other clients.

Results of studies are proprietary and belong to the End User. Members cannot share or use in any way any information learned from the conducting of research for an End User. All reasonable precautions must be taken to safeguard such information.

29. Will treat the respondent with respect and not influence a respondent's opinion or attitude on any issue through direct or indirect attempts, including the framing of questions.

Interviewers should not ask questions in a way that leads or influences respondents' answers, nor can they provide their own opinions, thoughts or feelings that might bias a respondent and therefore have an impact on the answers given.

30. Will ensure that all formulas used during bidding and reporting during the data collection process conform with the MRA Incidence Guidelines or with an incidence calculation formula agreed upon between the client and research provider(s).

Procedures must be implemented to confirm or verify that client specification is being followed. No deviations from specifications should occur without client approval. Any variation from specifications will require mutual consent.

31. Will make factually correct statements, whether verbal or written, to secure cooperation and will honor promises made during the interview to respondents.

Interviewers will not knowingly provide respondents with information that misrepresents any portion of the interviewing process such as length of interview, scope of task involved, any out-of-pocket expense the respondent may incur as a result of participating in the survey (e.g. cell phone fees), compensation, or intended use of the information collected.

32. Will ensure that all interviewers comply with any laws or regulations that may be applicable when contacting or communicating to any minor (under 18 years of age) regardless

of the technology or methodology utilized.

Researchers have a responsibility to provide any and all applicable information to interviewers regarding the legal and proper handling of respondents under 18 years old

33. Will not reveal any information that could be used to identify clients without their written authorization.

Proper authorization from a client should be in written format prior to or during the data collection process. This authorization must include that the information will only be used for research purposes.

34. Will ensure that companies, their employees and subcontractors involved in the data collection process adhere to reasonable precautions so that multiple surveys are not conducted at the same time with a specific respondent without explicit permission from the sponsoring company or companies.

Company policies or procedures must prohibit the practice of multiple screening or interviewing of a single respondent during any one interview. Any deviation of this policy will require the permission and mutual consent of both Client and Data Collector. Primary specifications must be adhered to within any study. No demographic or screening information that may be used for future or additional studies will be collected.

35. Will consider all research materials provided by the client or generated as a result of materials provided by the client to be the property of the client. These materials will be retained or disposed of as agreed upon with the client at the time of the study.

Research findings will not be released or published without consent of the Client. Research materials are the Client's property and are to be returned or disposed of as per the Client's instructions.

Storage of data, concepts, products and other materials, as well as data security, must be in strict compliance of the Client's instructions.

The Client will convey the procedures required, if any, for storage and retention of any materials related to the study for which they are contracted. These procedures relate to any products or materials that may be disseminated to the respondents during the course of study, as well as the final disposal of these materials after the study has been completed. Records or study materials that relate to the administration and calculation of the final data set will be maintained for an agreed upon period of time after the completion of a study. Any specific needs of the Client that require extended storage or extraordinary handling must be discussed with the data collection firm during the course of the study.

36. Will, as time and availability permit, give their client the opportunity to monitor studies in progress to ensure research quality.

Within reason, clients should be able to have full and ready access to the briefing and interviewing processes through either in-person or remote monitoring. Reasonable opportunity must be provided.

37. Will ensure that information collected during any study will not be used for any sales, solicitations or Push Polling.

Information provided by respondents in an opinion and marketing research study cannot be used for unrelated, non-research purposes such as direct marketing, non-consent list generation, credit rating, push polling, fundraising or other intrusive marketing or political activities.

38. Will respect that all information contained in a facility database or held by an independent recruiter is the sole property of these entities.

Information derived from a facility's database or from an independent recruiter has been developed by that facility as a business investment. Use of this information by any other party, whether to develop

an outside database or for any other use is strictly prohibited unless written permission has been obtained from the facility's owner or other authorized party.

39. Will follow all use restrictions imposed by the facility in order to ensure confidentiality for all parties.

Facilities take extreme precautions to ensure confidentiality for all clients and participants. It is critical that all clients respect the need for confidentiality by remaining in their designated or assigned areas at all times. Facility personnel must authorize any use of any other part of the facility not specifically assigned to the client. This includes, but is not limited to, the kitchen, copying/fax area, respondent or client waiting room, other focus or viewing rooms, usability labs, and private offices. It is the sole discretion of the facility to grant or deny permission in accordance with these codes.

40. Will not permit use of respondent contact information for re-contacting a respondent unless the respondent has been informed of this possibility at the time of the original research, and given their consent to be contacted.

In order to preserve trust in the research process, respondents must be fully informed of other contact possibilities, when they are known, at the outset of the original project.

41. For Internet research, will follow all federal, state and local laws regarding internet/online communications. This takes into account all opt-in/opt-out requests.

Internet research is subject to many laws and regulations at both the state and federal level. It is incumbent upon all members to be familiar with all laws and regulations applicable to their business and ensure that all such laws and regulations are followed exactly.

42. For Internet research, will be familiar with the already established guidelines from MRA, IMRO and ESOMAR, which include the definition of unsolicited e-mails.

Familiarity with the established guidelines set forth by MRA, IMRO and ESOMAR is each member's responsibility. These guidelines have been prepared to help advise marketing researchers in their conducting of studies via Internet research with the public and with other businesses. Access these guidelines at: http://www.mra-net.org/codes/internet_ethics_guidelines.PDF <http://www.imro.org/> http://www.esomar.nl/guidelines/internet_guidelines.htm

43. For internet research, will ensure that the Researcher's identity is disclosed to respondents.

The company conducting Internet research must identify itself to all potential respondents and provide appropriate contact information (email address, physical address, phone number, etc.). This is so respondents can easily verify the validity of a research project or make inquiries prior to participating.

44. For internet research, will post privacy policy statements online.

All privacy policy statements must be easy to find, easy to use and comprehensible.

45. For internet research, will not use any data in any way contrary to the provider's published privacy statement without permission from the respondent.

Data shall not be captured without respondent's consent. Doing so is in direct violation of the privacy rights stated in the Code and may violate the laws of a particular jurisdiction.

46. For internet research, will not send unsolicited email to those who have opted out.

The respondents' right to privacy is paramount and will be respected.

SECTION B: Sampling

Those who provide sample must adhere to all prior standards and in addition:

47. Must be prepared to comply with requirements and limitations placed on data usage by data owners, including list brokers and database compilers. These requirements and limitations include but are not limited to:

- ▶ required submission of questionnaire documents when requested
- ▶ limitations on use of sensitive material including data on children, medical conditions, financial information and other areas deemed as sensitive by the list provider or owner
- ▶ not using samples or lists for any purpose other than legitimate research purposes
- ▶ holding household and personal data contained in sample information in the same strict confidence as collected survey data and using it only for the purposes of stratification, selection or control of survey samples or in tabulation of aggregate results
- ▶ ensuring that information derived from the sample will not be used for individual marketing efforts. It is understood that no marketing action can be taken toward an individual respondent as a result of his/her survey information and/or participation as a survey respondent

Owners of the data that define the sample have collected and assembled this information and therefore have control of how it will be used. Buyers of such data, whether independent sampling companies or other researchers, are bound to adhere to all rules and regulations set forth by the data owners.

48. Will not misrepresent the impact of sample methodology and its impact on survey data.

Fair and honest information as to how sample methodology will affect survey data must be available to sample purchasers. This information must accurately represent likely outcomes and results as opposed to other available methodologies.

49. Will, upon request, disclose practices and methods used for generating, stratifying and selecting specific samples.

Information on how certain samples are created must be made available to researchers so that they can make informed decisions about sample purchase and use.

50. Will, upon request, identify the appropriateness of the sample methodology itself and its ability to accomplish research objectives.

Information as to the appropriateness of the sample methodology must be made available to sample purchasers. This information must accurately portray the sample's ability to attain the buyer's research objectives. As a research partner, the sampling provider must be prepared to advise about alternative sampling methods if appropriate.

51. Will protect the identity and confidentiality of research organizations and will not disclose information without consent except in compliance with a court order or other legal demand (e.g. discovery phase of a pending legal case).

In the course of obtaining appropriate sample, sample purchasers may have to reveal extensive proprietary or client information to the Sample Provider. Clients must enjoy the full protection of total confidentiality as it pertains to a study or studies and their businesses before, during and after the purchasing of sample.

52. Will compile, maintain and utilize Internet samples of only those individuals who have provided their permission to be contacted (opt-in) and who have a reasonable expectation that they will receive Internet invitations for opinion and marketing research purposes.

In order to maintain the integrity of Internet research, and to comply with many state and federal laws and regulations, only opt-in respondents will be utilized for Internet marketing research projects.

53. Will not employ any deceptive methods in obtaining sample. Sample Providers will not employ any techniques or technologies, actively or passively, to collect e-mail addresses without a respondent's awareness or permission.

In order to maintain the integrity of all research, and to comply with many state and federal laws and regulations, only opt-in respondents will be utilized for Internet marketing research projects. By definition, opt-in respondents knowingly participate in the collection of their information; their information is not captured by any clandestine means.

54. Will provide access to their privacy policy, which will be prominently displayed, for public review on each survey administered online.

As part of our respecting respondents' rights and privacy, all respondents must have access to a privacy policy that clearly states how the information they provide will be used. Such access must be provided at the time of every contact with a respondent.

55. Will offer respondents the choice with each survey to be removed (opt-out) from future Internet invitations.

As part of our respecting respondents' rights and privacy, all respondents must be given the opportunity at any time to opt-out of any further contact for Internet research. Therefore, every Internet survey must provide an easy to use and easy to understand means of opting out.

Those Using Sample....

56. Will, to the fullest extent possible on each project, counsel End Users as to the appropriateness of the sample methodology being employed. Ultimately, communication of critical information resides with the Research Provider working with the End User.

If it is the responsibility of the Research Provider to procure sample, it is also the responsibility of the Research Provider to ensure that any and all pertinent information about the sample that will affect the outcome of the study or its results be conveyed to the End User (e.g. sample derivation, use and effect).

57. Will be prepared to disclose to the Sample Provider the research objectives including the nature of such decision making and data uses, and will not knowingly misrepresent or mislead intent to any entity involved in the research process.

In order to recommend appropriate sample, it is necessary that the Sample Provider have access to certain information that might otherwise be deemed proprietary or confidential. Not disclosing such information, or not disclosing such information fully and completely, can have a negative effect on the recommendation of proper and appropriate sample and therefore on the outcome of the survey research.

58. Will adhere to policies and/or contracts set forth by sample providers governing the use of purchased and/or licensed sample resources or files.

Sample Providers may set forth certain contingencies for the use of the data they provide. Such contingencies may include (but are not limited to) respondent confidentiality, use of sensitive data, single/multiple use of sample, limits of re-use or resale of sample data, and other data management controls. Purchasers of sample must be prepared to adhere to all such contingencies whether via a verbal or written agreement.

59. Will offer respondents the choice with each survey to be removed (opt-out) from future Internet invitations.

As part of our respecting respondents' rights and privacy, all respondents must be given the opportunity at any time to opt-out of any further contact for Internet research. Therefore, every Internet survey must provide an easy to use and easy to understand means of opting out.

SECTION C: Tabulation and Data Processing

Those who are engaged in Tabulation and Data Processing must adhere to all prior standards and in addition :

60. Will inform Clients, at their request, of the quality control procedures the Data Processing Company has in place.

These quality control procedures may include, but are not limited to, verification of a coder's work and how often this is done, the percentage of surveys and questions that are checked or recaptured during data entry, and how skip patterns and invalid responses are treated if any data validation is done.

61. Will provide Client, at their request, with a clear statement in writing of the work involved with regard to the scope of the project, timing, and associated costs.

When providing a cost or a quotation, the Data Processing Company will include, at the client's request, a detailed description of the work that needs to be undertaken and the estimated time it will take to provide the client with all deliverables.

62. Will inform Clients, at their request, of the archiving and storage procedures the Data Processing Company has in place.

The Data Processing Company will inform their client of their archiving and storage procedures as they relate to paper questionnaires and electronic media. If these procedures differ from the client's needs, the client will provide in writing the special terms under which the Data Processing Company will store paper questionnaires and electronic media, when and how they can be destroyed, and the costs involved. If the client has not provided such special terms in writing at the Data Collection Company's customary time of destruction, the Data Collection Company must obtain the client's written consent to proceed.

63. Will inform clients, at their request, of the software (name, producer and version) that is being utilized for their work.

When requested, the Data Processing Company will inform their client as to exactly what software programs are being utilized in conjunction with their work. The data processing company will provide evidence when requested that they are licensed to use the software, and will indemnify the client from legal actions which might result from their use of the software..

APPENDICES

Professional Standards – Enforcement and Filing a Complaint

Sanctions

There are three levels of sanctions for violations:

1. Censure, that is, state strong disapproval to a violator by issuing an official letter of complaint.
2. Suspension of membership for a determined period of time, barring the member from membership privileges, such as advertising through MRA publications or participation in MRA programs and events.*
3. Expulsion from membership in the Association, making the loss of membership permanent.*

Censure requires member acceptance and agreement to rectify, improve and/or cease and desist as appropriate for the offense. Failure to act may result in suspension. The name of the censured party will appear in one issue of Alert! for the publication deadline closest to the final decision of the Committee. Details of Censures are not made public and remain confidential.

Suspension and Expulsion carry heavier penalties. To whit:

The names of members who have been suspended or expelled, and the outcome of their cases stating the Code points of which they are in violation, will be published in Alert! for a period of up to one year. Members under suspension lose all member benefits during the period of suspension and may not speak at any official MRA events (National or Chapter), and may not run for nor hold any MRA office. Expelled members or member companies face a lifetime prohibition from re-joining MRA.

Cumulative Violations

Multiple violations are viewed as cumulative and will be treated as follows:

1. Within a 5-year period, if a person or company accumulates 3 Censures, they will receive a one-year suspension.
2. Within a 5-year period, if a person or company accumulates 2 Suspensions, they will be expelled.
3. Within a 5-year period, if a person or company accumulates 1 or more Censures AND a Suspension, they will be expelled.

Definition of Membership Responsibility

All potential MRA members must sign the Code of Marketing Research Standards as a condition of membership. Failure to sign the Code precludes membership in MRA.

The Professional Standards Committee may censure, suspend or expel a company due to the actions of one or more employees even if the employee(s) in question are not members of MRA if the offense is the result of a company policy or pervasive action, explicit or implicit, that promotes or allows such punishable behaviors.

Complaints of alleged unethical behavior may be filed against an MRA member or member company who/that is suspected to have violated the Code. Such charges must be documented in writing using the official Complaint Form available on the MRA website, and forwarded to MRA's CEO/Executive Director. All related investigations are confidential, and the Professional Standards Committee members, the deliberators in such evaluations, will be reviewed for possible conflict(s) of interest in each case. A company or individual member found to be in violation of the Code may appeal the Professional Standards Committee findings to an objective arbitrator. MRA will NOT act on anonymous complaints.

Sanctions will be determined on a case-by-case basis, and will depend on the severity, nature, and cumulative amount of violations. Also considered will be whether such violations constitute a pattern that establishes the member to be incapable or unwilling to comply with the Code.

Complaint Filing and Review Procedures

A complaint is filed with MRA CEO/Executive Director identifying alleged improper conduct of a specific MRA member, outlining and identifying the specific section of the Code where the alleged violation occurred. The complainant supplies reliable documentation and personal knowledge of the alleged violation. The complaint must be received no later than 60 days from the end of the complainant's involvement in a study or a longer period of time as determined by the Committee after review on a case-by-case basis.

1. Via Certified Mail/signature required, the CEO/Executive Director notifies the complainant within 5 business days of receipt of the Alleged Violation Form.
2. The CEO/Executive Director immediately forwards the complaint to the Volunteer Chair of the Professional Standards Committee for review.
3. The Volunteer Chair of the Professional Standards reviews the complaint and ascertains if the materials constitute evidence of a violation against the MRA Code.
4. If they do not, the complainant is to be notified by certified letter of the Chair's findings within 30 days and the case is closed.
5. If the Chair determines that the materials might constitute evidence of a violation of the Code, the Chair calls a meeting of the Committee to determine whether the materials indicate a violation against the Code.
6. The Professional Standards Committee reviews the material and if it is determined not to be a violation, the complainant is to be notified by certified letter of the Committee meeting within 30 days and the case is closed. If the review determines it to be a violation, proceed to Step 7.
7. The Chair of the Professional Standards Committee begins a detailed investigation by notifying the person against which the complaint has been lodged (responding party) of the alleged violation and requests a written response to the allegation within 30 days from date of the Committee's letter to be sent by certified mail with signature required card. A copy is sent to the CEO/Executive Director.
8. The CEO/Executive Director receives the responding party's response and within 3 business days notifies the responding party in writing of receipt.
9. The CEO/Executive Director will forward the response within 3 business days to the Chair, Professional Standards Committee and the Committee.
10. The Professional Standards Committee meets as soon as possible to allow at least a three-fourths majority of the Committee to attend, and discusses the complaint and the materials received. This is done to determine the validity and the severity of the complaint. They then determine the next action steps.
11. The Professional Standards Committee notifies the complainant and the responding party by certified letter with signature required card of the Committee's decision, within 5 business days of decision.
12. If either party, complainant or responding party, disputes the decision of the Committee, then the Professional Standards Committee offers the opportunity to have an objective arbitrator hear the complaint.
13. MRA CEO/Executive Director selects the objective arbitrator in coordination with Professional Standards Committee Chair and materials are sent. The Arbitrator makes a decision. The Arbitrator announces the decision to the Professional Standards Committee and both parties. The non-prevailing party bears the full expense of the arbitrator's fees.

14. If the member's membership rights are suspended for a period of time or if the member is expelled from the Association, the final results are published in the Alert! Newsletter for a period up to one year as determined by the Professional Standards Committee. The results will be published in a manner at the discretion of the MRA CEO/Executive Director in concert with the staff editor of Alert!.

How to Comply With The Children's Online Privacy Protection Rule

The Children's Online Privacy Protection Act, effective April 21, 2000, applies to the online collection of personal information from children under 13. The rule spells out what a Web site operator must include in a privacy policy, when and how to seek verifiable consent from a parent and what responsibilities an operator has to protect children's privacy and safety online.

The Federal Trade Commission (FTC) staff prepared this guide to help operators comply with the requirements for protecting children's privacy online and understand the FTC's enforcement authority.

Who Must Comply

If you operate a commercial Web site or an online service directed to children under 13 that collects personal information from children or if you operate a general audience Web site and have actual knowledge that you are collecting personal information from children, you must comply with the Children's Online Privacy Protection Act.

- ▶ To determine whether a Web site is directed to children, the FTC considers several factors, including the subject matter; visual or audio content; the age of models on the site; language; whether advertising on the Web site is directed to children; information regarding the age of the actual or intended audience; and whether a site uses animated characters or other child-oriented features.
- ▶ To determine whether an entity is an "operator" with respect to information collected at a site, the FTC will consider who owns and controls the information; who pays for the collection and maintenance of the information; what the pre-existing contractual relationships are in connection with the information; and what role the Web site plays in collecting or maintaining the information.

Personal Information

The Children's Online Privacy Protection Act and Rule apply to individually identifiable information about a child that is collected online, such as full name, home address, email address, telephone number or any other information that would allow someone to identify or contact the child. The Act and Rule also cover other types of information -- for example, hobbies, interests and information collected through cookies or other types of tracking mechanisms -- when they are tied to individually identifiable information.

Basic Provisions

Privacy Notice

Placement

An operator must post a link to a notice of its information practices on the home page of its Web site or online service and at each area where it collects personal information from children. An operator of a general audience site with a separate children's area must post a link to its notice on the home page of the children's area.

The link to the privacy notice must be clear and prominent. Operators may want to use a larger font size or a different color type on a contrasting background to make it stand out. A link in small print at the bottom of the page -- or a link that is indistinguishable from other links on your site -- is not considered clear and prominent.

Content

The notice must be clearly written and understandable; it should not include any unrelated or

confusing materials. It must state the following information:

- ▶ The name and contact information (address, telephone number and email address) of all operators collecting or maintaining children's personal information through the Web site or online service. If more than one operator is collecting information at the site, the site may select and provide contact information for only one operator who will respond to all inquiries from parents about the site's privacy policies. Still, the names of all the operators must be listed in the notice.
- ▶ The kinds of personal information collected from children (for example, name, address, email address, hobbies, etc.) and how the information is collected -- directly from the child or passively, say, through cookies.
- ▶ How the operator uses the personal information. For example, is it for marketing back to the child? Notifying contest winners? Allowing the child to make the information publicly available through a chat room?
- ▶ Whether the operator discloses information collected from children to third parties. If so, the operator also must disclose the kinds of businesses in which the third parties are engaged; the general purposes for which the information is used; and whether the third parties have agreed to maintain the confidentiality and security of the information.
- ▶ That the parent has the option to agree to the collection and use of the child's information without consenting to the disclosure of the information to third parties.
- ▶ That the operator may not require a child to disclose more information than is reasonably necessary to participate in an activity as a condition of participation.
- ▶ That the parent can review the child's personal information, ask to have it deleted and refuse to allow any further collection or use of the child's information. The notice also must state the procedures for the parent to follow.

Direct Notice to Parents

Content

The notice to parents must contain the same information included on the notice on the Web site. In addition, an operator must notify a parent that it wishes to collect personal information from the child; that the parent's consent is required for the collection, use and disclosure of the information; and how the parent can provide consent. The notice to parents must be written clearly and understandable, and must not contain any unrelated or confusing information. An operator may use any one of a number of methods to notify a parent, including sending an email message to the parent or a notice by postal mail.

Verifiable Parental Consent

Before collecting, using or disclosing personal information from a child, an operator must obtain verifiable parental consent from the child's parent. This means an operator must make reasonable efforts (taking into consideration available technology) to ensure that before personal information is collected from a child, a parent of the child receives notice of the operator's information practices and consents to those practices.

The FTC utilizes a sliding scale approach to parental consent in which the required method of consent will vary based on how the operator uses the child's personal information. That is, if the operator uses the information for internal purposes, a less rigorous method of consent is required. If the operator discloses the information to others, the situation presents greater dangers to children, and a more reliable method of consent is required.

Internal Uses

Operators may use email to get parental consent for all internal uses of personal information, such as marketing back to a child based on his or her preferences or communicating promotional updates about site content, as long as they take additional steps to increase the likelihood that the parent has, in fact, provided the consent. For example, operators might seek confirmation from a parent in a delayed confirmatory email, or confirm the parent's consent by letter or phone call.

Public Disclosures

When operators want to disclose a child's personal information to third parties or make it publicly available (for example, through a chat room or message board), the sliding scale requires them to use a more reliable method of consent from parents, including:

- ▶ getting a signed form from the parent via postal mail or facsimile;
- ▶ accepting and verifying a credit card number in connection with a transaction;
- ▶ taking calls from parents, through a toll-free telephone number staffed by trained personnel;
- ▶ email accompanied by digital signature;

But in the case of a monitored chat room, if all individually identifiable information is stripped from postings before it is made public -- and the information is deleted from the operator's records -- an operator does not have to get prior parental consent.

Disclosures to Third Parties

An operator must give a parent the option to agree to the collection and use of the child's personal information without agreeing to the disclosure of the information to third parties. However, when a parent agrees to the collection and use of their child's personal information, the operator may release that information to others who uses it solely to provide support for the internal operations of the website or service, including technical support and order fulfillment.

Exceptions

The regulations include several exceptions that allow operators to collect a child's email address without getting the parent's consent in advance. These exceptions cover many popular online activities for kids, including contests, online newsletters, homework help and electronic postcards.

Prior parental consent is not required when:

- ▶ an operator collects a child's or parent's email address to provide notice and seek consent;
- ▶ an operator collects an email address to respond to a one-time request from a child and then deletes it;
- ▶ an operator collects an email address to respond more than once to a specific request -- say, for a subscription to a newsletter. In this case, the operator must notify the parent that it is communicating regularly with the child and give the parent the opportunity to stop the communication before sending or delivering a second communication to the child;
- ▶ an operator collects a child's name or online contact information to protect the safety of a child who is participating on the site. In this case, the operator must notify the parent and give him or her the opportunity to prevent further use of the information;
- ▶ an operator collects a child's name or online contact information to protect the security or liability of the site or to respond to law enforcement, if necessary, and does not use it for any other purpose.

New Notice for Consent

An operator is required to send a new notice and request for consent to parents if there are material changes in the collection, use or disclosure practices to which the parent had previously agreed. Take the case of the operator who got parental consent for a child to participate in contests that require

the child to submit limited personal information, but who now wants to offer the child chat rooms. Or, consider the case of the operator who wants to disclose the child's information to third parties who are in materially different lines of business from those covered by the original consent -- for example, marketers of diet pills rather than marketers of stuffed animals. In these cases, the Rule requires new notice and consent.

Access Verification

At a parent's request, operators must disclose the general kinds of personal information they collect online from children (for example, name, address, telephone number, email address, hobbies), as well as the specific information collected from children who visit their sites. Operators must use reasonable procedures to ensure they are dealing with the child's parent before they provide access to the child's specific information.

They can use a variety of methods to verify the parent's identity, including:

- ▶ obtaining a signed form from the parent via postal mail or facsimile;
- ▶ accepting and verifying a credit card number;
- ▶ taking calls from parents on a toll-free telephone number staffed by trained personnel;
- ▶ email accompanied by digital signature;
- ▶ email accompanied by a PIN or password obtained through one of the verification methods above.

Operators who follow one of these procedures acting in good faith to a request for parental access are protected from liability under federal and state law for inadvertent disclosures of a child's information to someone who purports to be a parent.

Revoking & Deleting

At any time, a parent may revoke his/her consent, refuse to allow an operator to further use or collect their child's personal information, and direct the operator to delete the information. In turn, the operator may terminate any service provided to the child, but only if the information at issue is reasonably necessary for the child's participation in that activity. For example, an operator may require children to provide their email addresses to participate in a chat room so the operator can contact a youngster if he is misbehaving in the chat room. If, after giving consent, a parent asks the operator to delete the child's information, the operator may refuse to allow the child to participate in the chat room in the future. If other activities on the Web site do not require the child's email address, the operator must allow the child access to those activities.

Timing

The Rule covers all personal information collected after April 21, 2000, regardless of any prior relationship an operator has had with a child. For example, if an operator collects the name and email address of a child before April 21, 2000, but plans to seek information about the child's street address after that date, the later collection would trigger the Rule's requirements. In addition, come April 21, 2000, if an operator continues to offer activities that involve the ongoing collection of information from children -- like a chat room -- or begins to offer such activities for the first time, notice and consent are required for all participating children regardless of whether the children had already registered at the site.

Safe Harbors

Industry groups or others can create self-regulatory programs to govern participants' compliance with the Children's Online Privacy Protection Rule [PDF]. These guidelines must include independent monitoring and disciplinary procedures and must be submitted to the Commission for approval. The Commission will publish the guidelines and seek public comment in considering whether to approve the guidelines. An operator's compliance with Commission-approved self-regulatory guidelines will

generally serve as a “safe harbor” in any enforcement action for violations of the Rule.

Enforcement

The Commission may bring enforcement actions and impose civil penalties for violations of the Rule in the same manner as for other Rules under the FTC Act. The Commission also retains authority under Section 5 of the FTC Act to examine information practices for deception and unfairness, including those in use before the

Rule’s effective date. In interpreting Section 5 of the FTC Act, the Commission has determined that a representation, omission or practice is deceptive if it is likely to:

- ▶ mislead consumers; and
- ▶ affect consumers’ behavior or decisions about the product or service.

Specifically, it is a deceptive practice under Section 5 to represent that a Web site is collecting personal identifying information from a child for one reason (say, to earn points to redeem a premium) when the information will be used for another reason that a parent would find material -- and when the Web site does not disclose the other reason clearly or prominently. In addition, an act or practice is unfair if the injury it causes, or is likely to cause, is:

- ▶ substantial;
- ▶ not outweighed by other benefits; and
- ▶ not reasonably avoidable.

For example, it is likely to be an unfair practice in violation of Section 5 to collect personal identifying information from a child, such as email address, home address or phone number, and disclose that information to a third party without giving parents adequate notice and a chance to control the collection and use of the information.

For More Information

If you have questions about the Children’s Online Privacy Protection Rule [PDF], visit the FTC online at www.ftc.gov/kidzprivacy. You also may call the FTC’s Consumer Response Center toll-free at 1-877-FTC-HELP (382-4357), or write Consumer Response Center, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Compliance with Government Legislation

It is expected that all researchers in general, and all MRA members specifically, will be informed about and comply with governmental acts and legislation that affect survey and opinion research.

MRA members should become familiar with these acts in their entirety. However, simplified references with key points stressed are provided for easy reference.

PLEASE NOTE: The information provided in this document is not intended and should not be construed as or substituted for legal advice. It is provided for informational purposes only. It is advisable to consult with private counsel on the precise scope and interpretation of any given laws/legislation and their impact on your particular business.

TCPA and TSR:

- ▶ Do NOT call a cell phone via autodialer without prior consent; there are potential regulatory implications.
- ▶ If you call someone on a land line and they give you a cell phone number to call back, you can then auto-dial the cell number (acts as a waiver of rights)
- ▶ You cannot use an auto-dialer to call a cell phone
- ▶ Neustar maintains updated database of numbers moved to/from cell phones

Restrictions on Telephone Solicitations	Telephone Consumer Protection Act	Telemarketing Fraud Act
Do-not-call-list provisions: Do they apply to unsolicited survey research calls?	No. The amended TCPA Rules supplements the FTC's national do-not call registry; restricting other categories of sales-related calls, as well as intra-state calls. Telemarketers are also required to comply with a request not to be called and under the amended Rules, must comply with such a request within 30 days and for a period of five years.	No. The amended FTC Rules requires telemarketers and telemarketers calling to solicit charitable contributions to comply with an individual's do-not-call request. In addition, telemarketers will be prohibited from calling numbers (residential and cellular) listed on a FTC national do-not-call registry.
Autodialer: Does the law or the agency regulations restrict the use of autodialers for survey research calls?	Yes (in part). "Automatic telephone dialing systems" (determined by the FCC in 2003 to include predictive dialers) cannot be used to call a 911 line, an emergency line of a hospital, a doctor's office, a health care facility, a poison control center, a fire department, a law enforcement agency, a paging service, a cellular telephone service where the called party is charged for the call* or in such a way that two or more telephone lines of a multi-line business are engaged simultaneously. The Amended Rules also address the issue of "call abandonment" (or "dead air") by telemarketers.	No. The use of automatic dialing equipment is addressed to some extent in the amended provisions of the FTC regulations, concerning "call abandonment" (or "dead air") by telemarketers.
Abandonment Rates: Do they apply to survey research calls?	No. The call abandonment provisions regulate sales-related calls only.	No. The call abandonment provisions regulate telemarketing calls only.
Time of Day Restrictions: Do they apply to survey research calls?	No. The 8am-9pm time-of-day restrictions are placed on sales calls only.	No. The 8am-9pm time-of-day restrictions are limited to telemarketers only.
Caller ID Restrictions: Do they apply to survey research calls?	No. The amended TCPA Rules prohibit telemarketers from blocking Caller ID, requires them to transmit Caller ID the Caller ID must permit the individual to make a do-not-call request during regular business hours.	No. The amended TSR prohibits the blocking of Caller ID by telemarketers, requires them to transmit their number and, when available, the firm's name.
Which federal agency implemented the law?	The FCC is responsible for implementing the law. The regulations can be found at 47 C.F.R. 64.1200.	The FTC is responsible for implementing the law. The regulations can be found at 16 C.F.R. 310. The amended FTC regulations can be found at: http://www.ftc.gov/os/2002/12/tsrfinalrule.pdf
Where can the law be found?	47 U.S.C.S. 227	15 U.S.C. 6101

CAN-SPAM:

CAN-SPAM points as to how to draft proper headings and how to avoid company emails being sent as spam or being labeled as commercial.

Things to avoid:

- ▶ . Don't use populated BCC/bulk mail fields (often predictive of spam)
- ▶ . HTML messages are more often spam than text messages
- ▶ . The color red seems to trip spam filters
- ▶ . Subject line keywords that are "sales-y" trip spam filters. These words include but are not limited to offer, free, cash, bargain, win, promo, reward, marketing. Survey research should avoid these terms under all circumstances.

Gramm-Leach-Bliley (GLB):

GLB provides for protecting the privacy of consumer information held by financial institutions. This is at the heart of the financial privacy provisions of the Gramm-Leach-Bliley Financial Modernization Act of 1999. The GLB Act requires companies to give consumers privacy notices that explain the institutions' information-sharing practices. In turn, consumers have the right to limit some - but not all - sharing of their information.

For a brief but more detailed look at the basic financial privacy requirements of the law, please visit this site: <http://www.ftc.gov/bcp/conline/pubs/buspubs/glbshort.htm>

Health Insurance Portability and Accountability Act(HIPAA):

The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule is the first comprehensive Federal protection for the privacy of personal health information (PHI).

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law (enacted in 1996, went into effect in April 2003), concerning the privacy of "protected health information" by "covered entities." As a general matter, survey research entities are NOT "covered entities" under HIPAA but can be indirectly covered/affected by the law/rules as "Business Associates."

The application of the law/rules on survey research is triggered when they obtain protected health information (PHI) from a "covered entity."

Information regarding HIPAA can be found at:

<http://hhs.gov/ocr/hipaa/whatsnew.html> and <http://www.cms.gov/hipaa/hipaa2/default.asp>

- ▶ Survey Researchers are Business Associates (BA) and therefore are restricted from disclosing PHI, except under certain circumstances
- ▶ Safeguards must be implemented to prevent unauthorized use or disclosure.

Among those are:

- ▶ Must detail who will have access to PHI
- ▶ Must establish computer password security measures
- ▶ Use secure servers, data encryption
- ▶ Agree to mitigate, to extent practicable, harmful effects of disclosure
- ▶ Business associates may disclose PHI if disclosure is required by law and use of PHI by the person receiving the PHI is restricted
- ▶ Essentially, BAs must take every precaution possible before disclosing PHI, and even then must try to limit how much PHI is disclosed, and to whom

IMRO STANDARDS

(with full detail and clarification)

Respondent cooperation is voluntary

Opinion and marketing researchers and their companies should avoid intruding unnecessarily on the privacy of Internet respondents. Survey respondents' cooperation should at all times be voluntary. No personal information unnecessary to the project, which is additional to that already available from other sources, should be sought from or about respondents without their prior knowledge and consent.

In obtaining the necessary agreement from respondents, the opinion and marketing researcher must not mislead them about the nature of the research or the uses that will be made of the findings. In order to prevent biased responses there may be occasions, however, when the purpose of the research cannot be fully disclosed to respondents at the beginning of the interview. The researcher should avoid deceptive statements that would be harmful or create a nuisance to the respondent; for example, the respondent should be told the likely length of the interview or about the possibilities of being re-interviewed on a later occasion. Respondents should also be told in advance if they might incur costs (e.g., as online time) if they cooperate in the survey. Respondents may request at any time during or after the interview that part or all of the record of their responses be destroyed or deleted and the opinion and marketing researcher must conform to any such request where reasonable. (*Refer to Council for Marketing and Opinion Research: Respondent Bill of Rights at www.cmor.org*)

Researcher's Identity Should Be Disclosed to Respondents

The company conducting Internet research should identify itself to all potential respondents and provide appropriate contact information (email address, physical address, phone number, etc.). This is so respondents can easily verify the validity of a research project or make inquiries prior to deciding to participate in the study or survey.

Respondents' Rights to Anonymity Should Be Safeguarded

Unless respondents give their verifiable informed consent to allow themselves to be identified with the information they are providing, opinion and marketing research companies should ensure that the respondents' anonymity is safeguarded. Opinion and marketing research companies should further ensure that the information provided by respondents is used only for the research study in which each respondent consented to participate. Information provided by respondents in an opinion and marketing research study cannot be used for unrelated, non-research purposes such as direct marketing, non-consent list generation, credit rating, push polling, fund-raising or other intrusive marketing or political activities.

Privacy Policy Statements Should Be Posted Online

Researchers should post their privacy policy statement on their online site. When such privacy policy statements exist, they should be easy to find, easy to use and comprehensible.

- ▶ Notice – Disclose their information practices before collection of personal information from individuals.
- ▶ Choice – Give individual options with respect to whether and how personal information collected about them may be used for purposes beyond those for which the information was provided.
- ▶ Access – Individuals should be able to view and contest the accuracy and completeness of data collected about them. The Federal Trade Commission (FTC) has acknowledged that

the access requirement will vary from site to site, business to business, taking into account various types of businesses.

- ▶ Security – Take reasonable steps to assure that information collected from individuals is accurate and secure from unauthorized use.
- ▶ Enforcement – The use of a reliable mechanism to impose sanctions for noncompliance with these fair information practices.

Data Security Should Be Maintained

Companies conducting Internet opinion and marketing research should be able to provide adequate security for both respondents and clients in the transmission and storage of information and data. All reasonable precautions should be taken to secure and protect computer servers and databases from unauthorized access to proprietary files and information.

Reliability and Validity of Findings Should Be Disclosed to the Public

Clients and other users of opinion and marketing research and the general public should not be in any way misled about the reliability and validity of any Internet research findings. Researchers should:

- ▶ Follow scientifically sound sampling methods consistent with the purpose of the research;
- ▶ Publish a clear statement of the sample universe definition used in a given survey, the research approach adopted, the response rate achieved and the method of calculation;
- ▶ Publish any reservations about the possible lack of projectability or other limitations of the research findings, for instance resulting from non-response and other factors.

It is equally important that any research about the Internet (e.g., to measure penetration, usership, etc.) that employs other data collection methods, such as telephone or mail, also clearly refers to any sampling or other limitations on the data collected.

Researchers Interviewing Minors Should Adhere to the Children's Online Privacy Protection Act

Opinion and marketing research companies conducting surveys or studies with minors should adhere to the Children's Online Privacy Protection Act (COPPA) set by the Federal Trade Commission (FTC). The Act applies to the online collection of personal information from children under 13 years old.

COPPA applies to individually identifiable information about a child that is collected online, such as full name, home address, email address, telephone number or any other information that would allow someone to identify or contact the child. The Act also covers other types of information - for example, hobbies, interests and information collected through "cookies" (an attachable unique identifier to a person's preferences on a Web site) or other types of tracking mechanisms - when they are tied to individually identifiable information.

Before collecting, using or disclosing personal information from a child, the researcher must obtain verifiable parental consent from the child's parent. This means an operator must make reasonable efforts (taking into consideration on available technology) to ensure that before personal information is collected from a child, a parent of the child receives notice of the operator's information practices and consents to those practices.

The researcher must post a link to the privacy policy on the home page of its Web site and in each area where opinion and marketing researchers collect personal information from children. The link to the privacy notice must be clear and prominent. (For more information refer to section IV in this Ethical Guideline about privacy policies). You can visit the FTC Web site at www.ftc.gov for the full text of COPPA.

The notice must be clearly written and comprehensible. It should not include any unrelated or confusing materials.

It must provide the following information:

- ▶ The name and contact information (address, telephone number and email address) of all researchers collecting or maintaining children's personal information through the Web site or online service. If more than one researcher is collecting information at the site, the site may select and provide contact information for only one researcher who will respond to all inquiries from parents about the site's privacy policies. Still, the names of all the researchers must be listed in the notice.
- ▶ The kinds of personal information being collected from children (e.g., name, address, email address, hobbies, etc.) and how the information is collected - directly from the child or passively, say, through "cookies."

If the researcher discloses information collected from children to third parties, then the researcher also must disclose:

- ▶ The kinds of businesses in which the third parties are engaged;
- ▶ The general purposes for which the information is used;
- ▶ Whether the third parties have agreed to maintain the confidentiality and security of the information;
- ▶ That the parent has the option to agree to the collection and use of the child's information without consenting to the disclosure of the information to third parties.

The researcher may not require a child to disclose more information than is reasonably necessary to participate in an activity as a condition of participation. The parent can review the child's personal information, ask to have it deleted, and refuse to allow any further collection or use of the child's information. The notice also must state the procedures for the parent to follow. (*Refer to the FTC Web site at www.ftc.gov for more information*)

Unsolicited Email Should Not Be Sent to Those Requesting Not to Receive Any Further Email

Overall, researchers by should acknowledge respondents' rights to privacy by:

- ▶ Specifically offering the potential respondent the opportunity to "opt-out" or be removed from an email list;
- ▶ Not sending unsolicited messages online to respondents who have indicated they do not wish to receive such messages relating to a research project or any follow-up research resulting directly from it;
- ▶ Not collecting email addresses under the guise of some other activity or by some means that does not allow the respondent to be aware of this.

All email messages to respondents will carry the researcher's valid reply-to address and will clearly state the purpose of the message in the email subject heading. Research companies will honor the respondents' rights to request that they receive no further email contact.

POSITION PAPERS

From time to time there may be topics that are of interest or concern to the Marketing Research profession. These topics may encompass issues that affect Marketing Research in some way, yet some of these issues may not be fully integrated into our day-to-day businesses. Others may be controversial or unresolved. Therefore, the issues surrounding these topics do not at this time warrant becoming a part of our Code of Marketing Research Standards. However, these topics are considered important enough to justify MRA's taking a position on them.

MRA will be presenting Position Papers on topics that merit such attention. As these and other topics evolve over time, MRA will be poised to incorporate new information into existing Position Papers or create new Position Papers. If and when it is appropriate, MRA will evaluate the need to address relevant issues in the Code of Marketing Research Standards.

MRA POSITION PAPER**MYSTERY SHOPPING**

Mystery Shopping is a long-established research technique used by a wide variety of commercial, governmental and other organizations. Its purpose is to help such (groups) to assess and improve the standards of service they provide to their customers by comparing their achieved performance against their own targets and against the standards provided by competitors and other organizations. The approach involves the use of evaluators who are specially trained to observe and measure the nature and quality of the services being offered to customers.¹ These evaluators, or Mystery Shoppers, pose as consumers and chronicle detailed information about their Mystery Shopping experience using questionnaires or narrative reports.

Mystery Shopping is used not only by Marketing Researchers but also by merchandisers, security firms, private investigators and employee training groups and organizations.

Provided that it is carried out professionally and with appropriate safeguards, Mystery Shopping is a valid and legitimate form of marketing research. It does have certain unique characteristics that distinguish it from other types of research. In particular, “respondents” are not aware that they are the subjects of research.² Also, contrary to other Marketing Research standards, identifying the respondent’s name to the sponsor is usually part of the process. This is because one of the most common uses of Mystery Shopping is to evaluate a company’s training program as it relates to customer service delivery. An individual respondent’s performance may be assessed as part of the process. Additionally, it is not unusual for companies to use the outcome of Mystery Shopping as a way to identify employees who need further training or who deserve bonuses or rewards.

MRA considers Mystery Shopping a legitimate form of Marketing Research when it is employed for Customer Satisfaction purposes; that is, to determine likely customer perceptions and needs. It is not considered Marketing Research when it is used for non-research purposes such as identifying individuals for disciplinary actions, falsely elevating sales by creating a demand for products or services that does not really exist in the current marketplace or obtaining personal information for non-research purposes.

For further information on Mystery Shopping, consult these resources:

ESOMAR “Guidelines on Mystery Shopping” at <http://www.esomar.nl/guidelines/mysteryshopping.htm>

Mystery Shopping Providers Association at www.mysteryshop.org

¹ ESOMAR “Guidelines on Mystery Shopping”

² Ibid

MRA POSITION PAPER**SALES WAVES**

Sales Waves are respondent contacts that take place immediately upon the conclusion of a Marketing Research interview or in successive waves thereafter.

A Sales Wave offers to the respondent the product or service that was the subject of the initial interview. The product or service is made directly available to the respondent at the regular or expected retail price and then is delivered to the respondent after money is exchanged via cash or the setting up of an account in the respondent's name. Almost always, at the conclusion of the Sales Wave portion of a study, all monies are returned to the respondent or the account is never collected upon.

The purpose of Sales Waves is to gauge actual purchase intent and, ultimately, likely sales volume. Data gathered from Sales Waves are considered more reliable than data gathered from hypothetical purchase intent questions because the respondent is making an actual commitment with his or her own dollars. It is a discrete choice test where respondents can receive the product or service of their choice or, perhaps, no product or service at all. In this scenario it is essential that respondents have the mind-set that they are paying real dollars for whatever they order.

Sales Waves are considered by some manufacturers and service providers to be essential in Marketing Research projects that involve new food products, breakthrough products or services, or line extensions. Because the intent is to generate information and not sales, Sales Waves are considered legitimate Market Research. The controversy arises over respondent perceptions of sales vs. research: can respondents make this subtle but important distinction? There seem to be contradictions in the standard Marketing Research practice of utilizing Sales Waves. We make promises to respondents that we will not sell them anything and then we offer a product or service for sale at the end of the interview (or at sometime thereafter). Marketing Researchers have worked diligently to differentiate between selling and researching; "sugging", or Selling Under the Guise of Research is considered a violation of research ethics. However, there is a clear distinction in the motivation or underlying reason for sales vs.

Sales Waves: sales are employed to generate profits; Sales Waves are employed to generate data and information. Measuring expected sales or sales volume is a legitimate Marketing Research outcome.

It is the position of MRA that Sales Waves represent a legitimate Marketing Research technique. However, extreme care must be taken to safeguard the integrity of the Research process and the privacy of respondents. It is recommended that before MRA members accept a study involving Sales Waves they include the following questions in their discussion of the project with their client:

- ▶ Will all of the respondent's money be returned (or never collected on the established account) at the conclusion of the Sales Waves?
- ▶ Will product fulfillment be the responsibility of the manufacturer, and if so, how will respondent confidentiality be safeguarded?
- ▶ Will respondents receive an explanation of the Sales Wave process at the conclusion of the study so that they can be assured that this process was for information and not for profit?

With recent concerns over respondent cooperation and privacy, Sales Waves are not used as often as they once were. However, they continue to be used in our industry by many large manufacturers and service providers. Ultimately, the decision as to whether to accept studies that incorporate Sales Waves is a business decision that must be made by our members on a case-by-case basis.

MRA POSITION PAPER

Auto-Dialing Systems with CATI

The Current State of Affairs

The use of automatic dialing equipment in survey call centers has increased dramatically in recent years. Once used almost exclusively by the telemarketing industry, dialing systems have become a significant part of marketing research survey systems as a means for paring time and costs from call center data collection operations.

This paper is intended to discuss the issues pertaining to automatic dialing equipment and recommend adoption of standards for the Marketing Research Association.

Without an automatic dialing system, interviewers using a normal CATI system are required to dial each telephone number manually. The numbers may be provided on a paper list, or may be automatically displayed on the screen at the beginning of the survey. In each of these situations, inefficiencies caused by the interviewer can include:

1. Pausing longer than necessary prior to dialing the next number;
2. Dialing incorrect numbers; and
3. Recording an incorrect call disposition code.

The time waiting for a call to be answered—to be picked up by voice mail or an answering machine, or to ring a set number of times without being answered—is a major factor that leads to unproductive costs.

Automatic Dialing Technology

With the advent of the modem, which made it possible for computer software to automatically dial a telephone number, CATI systems were capable of causing the telephone number to be dialed by the system without the intervention of the interviewer. As a first step in auto-dialing, modems allowed CATI systems to control the pause between calls and ensured that a correct number was always dialed. However, the interviewer was still required to listen for the call to be answered, and then to enter the proper disposition code into the system.

Today, further efficiencies are achieved by more sophisticated equipment known as power dialers and predictive dialers. Not only does this equipment dial telephone numbers, it can also “listen” to the ringing process and determine if the call is answered by a real person, by an answering machine or a fax machine; is busy; or is not connecting to a working number. In addition, these types of systems can automatically pass the appropriate call disposition code back to the CATI system, all without ever involving the interviewer in the process. Such a process means that dialing equipment can now handle the entire calling process, leaving only the actual survey process to the interviewers. The dialer makes calls independently until a respondent is reached, and only then does it turn the call over to an interviewer.

A power dialer is a system that does not begin dialing numbers until an interviewer is available and ready to take a live call. Basically, the dialer determines when each

interviewer becomes available and only then begins dialing numbers until a live respondent is reached, and then passes the call to the interviewer. The interviewer waits until a call comes through, leaving all unsuccessful dials to be handled automatically behind the scene. With Power Dialers, a respondent is always passed immediately to an interviewer.

(Note: A variation on power dialing, called **preview dialing**, is a system that allows an agent to preview some aspect of the number to be called before allowing the dialer to begin attempting the

call. In most cases, this variation is used only by telemarketers, since research methodologies do not lend themselves to such intervention by interviewers.)

Predictive dialers take the additional step of attempting to eliminate the wait while the telephone is ringing by using a sophisticated algorithm to predict when an interviewer will likely become available, and dialing ahead of time, so that a live respondent is ready to speak as soon as the interviewer is ready for the next call. Predictive algorithms use factors such as the average length of an interview, incidence or connect rates, the number of interviewers working, the number of rings to wait, and the previous call history for the specific telephone number, to determine how many dialing attempts to be working on at any given moment in time. The ideal process is to reach a live respondent just as an interviewer finishes with a call and becomes available to take the next call. Even if an interviewer waits a few seconds before a live respondent is located, the overall reduction in wait time can be significant for large call centers. The combination of extremely accurate dialing and disposition coding, plus the reduced wait time, can result in significant cost savings.

The Problem of Abandoned Calls

However, with any predictive algorithm, the potential exists for an unusual string of successful call attempts to result in live respondents being reached when no interviewers are available to take the calls. Furthermore, the complexities associated with maintaining a continuous flow of available callers because of break times, post-call wrap-up work, varying call lengths, and other personnel issues further increase the potential of not having an interviewer available to take a call. In such cases, several alternative actions are common. One is to simply hang up or abandon the call. Other systems may play a prerecorded message asking the respondent to hold momentarily, or they simply put the call on hold hoping that an interviewer will become available before the respondent hangs up. Companies in the telemarketing industry are notorious for setting their predictive algorithms such that their sales people never wait more than a few seconds for a live respondent. The result is that many calls are abandoned, leaving the respondents angry and upset at having been bothered for no apparent reason. Some assume that someone is calling to determine if they are home or not before breaking in.

Consumer Response to Auto Dialers

Auto dialing technology in use by the telemarketing industry did not stop with predictive dialing and abandoned calls. In an ever increasing demand to allow agents to handle more and more calls, the telephony systems developed schemes to enable one agent to handle multiple calls simultaneously. The resulting impersonalization of unsolicited calls became a major source of frustration. Ultimately, the public responded by forcing the

U.S. governments to pass the National Do Not Call legislation, which led to the creation of the Do Not Call Registry, and a significant reduction in telemarketing calls.

Since marketing and opinion research services are exempt from the DNC policies, automatic dialers continue to offer significant cost savings for many call centers. Virtually all CATI systems on the market today include an automatic dialing option, either as a proprietary system, or as an open system that supports a variety of different auto dialer vendors.

Recommendations

As a part of our continuing effort to maintain a high degree of professionalism and public acceptance of the research process, the Marketing Research Association recognizes the importance of establishing a set of standards that will differentiate the use of dialing technology by members of the research community from others who do not care about the negative impact of inappropriate dialing practices.

The following recommendations should be considered when employing automatic dialing equipment in the research process:

1. When auto dialing systems are preferred, power dialing is the preferred methodology.
2. Any process that results in abandoned calls should be avoided or carefully managed to ensure that abandoned calls are extremely rare.
3. Predictive dialing should only be used when a sufficiently large number of interviewers are working on the project, such that the predictive algorithm can function effectively.
4. Predictive dialing should only be used when the system allows the abandonment rate to be set to 1 or less calls per 100 connected attempts.
5. If a call attempt results in an abandoned call, the associated telephone number must be flagged so that any further attempts to call that number must be made without any possibility of being abandoned a second time.
6. Predictive dialing should be used only when a report of abandoned calls is produced frequently and is reviewed by project managers regularly to ensure that the system is working properly. Periodic management audits of abandoned calls must be made to ensure that the system is functioning properly and is being used ethically.
7. Predictive dialing should only be used only when the variables required by the predictive algorithm to establish a dialing rate appropriate for the prescribed abandonment rate are provided accurately by the system that drives it. For example, if the prior call history for each number is necessary for the algorithm to function correctly, the CATI system's sample-management process must supply that information along with each telephone number.

The overall objective of these standards is to create an atmosphere in which predictive dialing is used responsibly and is properly managed, to prevent inadvertent misuse of the system. The Marketing Research Association understands that predictive dialing systems are already prevalent enough that the association cannot recommend against their use. It is the organization's hope that members of the research community will recognize the gravity of unethical usage in undermining public support for the research industry, and will adhere to standards that minimize the negative potential on the industry's success.

MRA POSITION PAPER

TRANSACTION-BASED CUSTOMER SATISFACTION CONFIDENTIALITY

Background

Customer satisfaction research is a long-established field of marketing research, which is used by a wide variety of business organizations. A specialized area within this field is transaction-based customer satisfaction. In transaction-based customer satisfaction research, customers are called shortly after using a company's product or service. The purpose of transaction research is to help the client firm assess and improve its customer service.

Discussion

Transaction-based customer satisfaction is especially prevalent and important where new more efficient technology, processes, budgets and work force changes are affecting customer service. The purpose of this research is to use the 'voice of the customer' to fine-tune customer service processes, so that internal client company changes result in optimal customer service. The analysis involved in this form of research is done by statistically comparing customer responses to internal records for the same events. Occasionally during this analysis, client company employees contact the customer for additional information concerning their service transaction. The focus of such contact is understanding and improving service and products, not marketing or sales.

In transaction-based customer satisfaction research, confidentiality is not expected because data collection is tied to a specific customer service event and the respondent is told during the survey that the purpose of the research is to improve the customer's future service. In this type of research, confidential customer responses are not shared outside the client company.

In addition, some industries conducting transaction-based customer satisfaction research are regulated by federal and state government bodies. An example of such an industry is telecommunications. In regulated industries, government agencies sometimes focus upon dissatisfied customers and require the regulated companies to

resolve customer issues. As a result, regulated companies cannot keep confidential customer responses from government bodies.

Summary

Confidentiality is important to marketing research and must be maintained. An exception to this confidentiality rule is transaction-based customer satisfaction research. In transaction-based customer satisfaction research, strict confidentiality is not possible because:

1. The customer and client are following-up on a specific transaction/event in order to improve future service. In this situation, the customer and client are working together toward a common purpose and confidentiality within the client company is not expected.
2. In regulated industries, government regulation often does not permit satisfaction research to remain confidential.