AMSRS
Australian
MARKET & SOCIAL RESEARCH SOCIETY

CASRO®
The Voice and Values of Research

MRS Evidence Matters™

Mobile Research Guidelines

September 2014

AMSRS, CASRO and MRS are part of the Global Research Business Network.

GLOBAL RESEARCH
BUSINESS NETWORK
APRC • EFAMRO • ARIA

www.grbn.org

Table of Contents

1. Introduction

The emergence of mobile technology has transformed the way people communicate and is rapidly becoming the preferred mode of telephone communication globally. Market, opinion and social researchers have already devised and applied numerous research approaches using mobile technology. It is the goal of these guidelines to promote standards and best practices for mobile research.

These guidelines cover mobile market research and provide contemporary guidance for research organizations. They also acknowledge that mobile research occurs in a dynamic environment. Accordingly these guidelines seek to establish ethical principles that research organizations can apply to specific technologies and methods as they emerge and develop.

It is important to note that these guidelines are based on the AMSRS Code of Professional Behaviour, the CASRO Code of Standards and Ethics and the MRS Code of Conduct. These codes provide a broad foundation that covers the fundamental ethical and professional principles that govern all forms of research and separate research from marketing, sales, and advertising. This document underscores the need to maintain the distinction between market, opinion and social research, and marketing/PR activities in mobile research as in all other research modes and methodologies.

Throughout these guidelines we use “must” when describing a principle that researchers are required to implement in order to comply with the AMSRS, CASRO and MRS codes previously cited. We use “should” when describing a principle that researchers may implement in different ways depending on the research design in question.

This document also recognizes that governmental regulations in this area are evolving and that there may be different laws and regulations in different countries. Therefore, these guidelines are based on the principles underlying current laws and regulations in different countries with respect to privacy and data protection, and intellectual property. It is critical for researchers to comply with all applicable governmental regulations and laws and be aware that even stricter standards and rules may apply in other jurisdictions, including the regional, national or international level.

In summary, these guidelines have been written to satisfy several needs: (a) to be consistent with the spirit and intent of existing laws; (b) to reflect the industry’s ethical and professional principles set out in our professional codes and (c) to be sufficiently broad and flexible to address both current and anticipated trends in mobile research.

2. Key Common Ethical Principles

These Mobile Research Guidelines are based on the common ethical standards that are applicable to all forms of research and are laid out in the codes of AMSRS, CASRO and MRS. The full set of principles and fundamental concepts are set out in Appendix 1. The key common ethical principles for research can be summarized as follows:

2.1. Distinguishing Market, Opinion and Social Research from Other Purposes

Research organizations must not permit personally identifiable information they collect in a research project to be used for direct marketing, sales, or advertising or permit any direct action to be taken toward an individual based on his or her participation in research. Disclosure of any personally identifiable information must be in accordance with the limitations and responsibilities described in the applicable industry association codes.

2.2. Voluntary Participation

Where participants and researchers **directly** interact, informed consent must be obtained in accordance with applicable privacy and data protection laws, regulations and relevant code. In all situations where informed consent must be obtained, participants must understand the purpose and use and voluntarily choose to participate.

2.3. Transparency

With mobile market research, transparency to the research participant is critical. Research organizations must disclose all applicable information about their activities to research participants in a timely and open manner and must provide details on how the researcher uses and shares the participant’s information.

2.4. Confidentiality

Research organizations are responsible for protecting the disclosure of participant data to third parties, including clients and members of the public. This includes the identity of individual research participants as well as their personally identifiable information. This information can only be shared if the participant expressly requests or permits such disclosure.

2.5. Privacy

Research organizations have a responsibility to strike a proper balance between the need for research in contemporary life with the privacy of individuals who become the participants in the research.

2.6. Avoidance of Harm

Research participants will be protected from unnecessary and unwanted intrusions and/or any form of personal harassment.

2.7. Professionalism

Researchers must exercise independent professional judgment and at all times apply their skills to the best of their ability.

2.8. Compliance with the Law

Research organizations must comply with existing local, national, and international law and regulations governing privacy, data protection, data security and the disclosure, receipt and use of personally identifiable information or personal data. In particular, researchers must establish a clear legal basis for the processing of personal data, especially where data is not obtained directly from the individual participant. Of special consideration is the compliance with legal requirements (e.g., US-EU Safe Harbor requirements, Binding Corporate Rules or applicable contractual provisions) relating to the international transfer of personally identifiable information or personal data. Also applicable are considerations as to whether the country to which the data is transferred offers an adequate level of data protection.

3. Scope

These guidelines cover the collection of data with mobile technology (including basic mobile phones, feature phones, smartphones, tablets and other mobile devices) for market, opinion or social research purposes. These guidelines cover research using browser-based and native applications. This includes video and voice data collection as well as passive data collection. These guidelines also apply to research conducted by using voice or text message (SMS) to contact respondents on their mobile phones.

These guidelines offer interpretation of rules and provide additional best practice information. They do not create new rules or legal obligations.

4. Distinguishing Between Research and Non-Research Activities

Just as with all research it is required in mobile research to distinguish between research and non-research activities. In some cases, those taking part in research could be exposed to sales and PR messages as part of the research process. This is permissible provided the purpose is for research and the applicable industry codes permit it. In situations where participants are exposed to sales and PR messages for purposes other than research, these activities cannot be referred to as research.

Research organizations must be transparent in their dealings with mobile market research participants, and not represent as market research any project that has another purpose. To promote clarity and protect the reputation of both the researcher and market research, the research services (and the organization or company carrying them out) must be presented in such a way that they are clearly differentiated from any non-research activities. To ensure the public is not confused when mobile research data are being used by an organization involved in both research and non-research activities, it is recommended that:

- the company's privacy policy and promotional literature differentiate the different services that are being offered, and clearly separate market research from other activities;

- it be easy for participants and others to contact the research organization carrying out the research;

- people making inquiries not encounter obstacles or organizational structures that create confusion about research sponsorship (e.g., by having to interact with a non-research organization or deal with non-research staff when they raise queries or complaints about market research activities); and

- the introduction used when contacting a participant clearly defines the purpose, never leaving the impression that the exercise has a research purpose if it does not.

These requirements do not prevent research organizations from being involved in non-research activities, provided that the purpose of collecting personally identifiable data is not misrepresented. Further, they do not in any way restrict the right of the organization to promote the fact that it carries out both market research and other activities, provided that the activities are clearly differentiated and conducted separately, in a manner consistent with the relevant laws and applicable research association codes.

Finally, when research organizations engage in non-research marketing activities, these activities must be conducted in a manner consistent with relevant laws and applicable marketing association codes. These activities and any associated websites, software applications and forums must be clearly labeled so as to permit participants, clients, legislators and regulators to easily understand what is a research activity and what is a non-research activity.

5. Definitions

Throughout these guidelines, there are a number of specific terms, with the following meanings:

5.1. App data – Data generated by or associated with a computer software application.

5.2. Client – An individual, organization, company, department or division, internal or external that requests, commissions or subscribes to a research project.

5.3. Confidentiality - A set of rules or a promise that limits access or places restrictions on certain types of information.

5.4. Cookies - Cookies are text files containing small amounts of information, which are downloaded to a computer, mobile device or other device when a user visits a web site. Cookies are then sent back to the originating web site on each subsequent visit, or to another web site that recognizes that cookie. Cookies are useful because they allow a web site to recognize a user's device.

Cookies serve many different functions that include making website navigation more efficient, remembering user preferences, and generally improving the user experience. They can also help to ensure that offers a user gets online are more relevant to them and their interests.

5.5. De-duplication – For access panels, a process to remove individuals who are registered more than once on the same access panel so they are included and represented only once. For sample surveys, a process to remove individuals who attempt to complete a survey or are offered a survey more than once. This can occur if a panelist or survey respondent is a member of more than one panel or sample source (panel or sample source overlap) and is selected to participate in a survey that is split across sample sources or fails to recall previously participating in a given survey.

5.6. Device ID - A technology-enabled system that establishes a set of configuration data about a respondent's device (computer, smartphone, etc.), which it transforms to create a "machine" or device fingerprint. Such systems assume the “machine fingerprint” uniquely identifies a device using device settings and characteristics associated with an individual device or, potentially, an individual user account. Device ID systems apply to computers, mobile devices, and other devices accessible via the Internet where surveys can be completed.

Note: Device ID is also referred to as digital fingerprinting and browser fingerprinting

5.7. Geolocation - The identification of the real-world geographic location of an object, such as a mobile phone or an Internet-connected computer. Geolocation may refer to the practice of assessing the location or to the actual assessed location.

5.8. Geo fencing – Assigning a virtual perimeter around a geographic location

5.9. Geo validation – Process of validating a geographic location that is recorded or reported.

5.10. GPS (Global Positioning System) - A space-based satellite navigation system that provides location and time information in all weather conditions, anywhere on or near the Earth where there is an unobstructed line of sight to four or more GPS satellites.

5.11. Informed Consent – Agreement by a respondent or participant to participate in research, made with complete knowledge of all relevant facts, such as the risks involved or any available alternatives. Consent may be withdrawn by the respondent at any time. Such agreement can be collected in written or electronic form. A record of the agreement, how it was obtained and the date and time the agreement was obtained must be kept.

5.12. Market Research – the systematic gathering and interpretation of information about individuals or organizations using the statistical and analytical methods and techniques of the applied social sciences to gain insight or support decision making. The identity of the research participant is never revealed to the user of the information without the participant's explicit consent. In addition, no sales, marketing, or advertising approach is made to participants as a direct result of their having provided any information.

5.13. Mobile Market Research - Any research done on a mobile phone or mobile device; wherever people may be - at home, work, out, abroad, etc.

5.14. Mobile Device – A mobile device (also known as a handheld device, a tablet or simply a handheld) is a small, hand-held computing device, typically having a display screen with touch input and/or a miniature keyboard and weighing less than 2 pounds / 0.9 Kg.

5.15. Mobile Phone - A mobile phone (also known as a cellular phone, cell phone and a hand phone) is a device that can make and receive telephone calls over a radio link while moving around a wide geographic area. There are three types of mobile phones:

- **Basic Mobile Phone -** A mobile phone with few or no features beyond basic dialling and messaging.

- **Feature Phone -** A feature phone is a mobile phone that has less computing ability than a smartphone, but is Internet enabled and has additional functions over and above a basic mobile phone. It is intended for customers who want a lower-price phone without all the features of a smartphone.

- **Smart Phone -** A smart phone is a mobile phone built on a mobile operating system, with more advanced computing capability and connectivity than a feature phone.

5.16. Mobile applications (available on feature phones and smart phones) – There are two basic types of mobile applications: native mobile apps and mobile web apps:

- **Native mobile app:** A native mobile app is an application that is coded in a specific programming language for a specific mobile device operating system. Native mobile apps are typically downloaded to a mobile device and provide fast performance and a high degree of reliability. They also have direct access to and a high level of control over a mobile device's features such as its camera. In addition, native apps have the capability to be used without an Internet connection.

- **Mobile Web app:** A mobile Web-based application that is accessed over a network connection using HTTP, rather than existing within a device's memory. Mobile web applications often run inside a Web browser. However, mobile web applications also may be client-based, where a small part of the program is downloaded to a user's mobile device, but processing is done over the Internet on an external server. While some mobile web apps can access mobile device features such as its camera, the level of control isn't at the same level as that of a native mobile app.

5.17. Passive Data Collection – In the context of mobile market research, the capture of data from a respondent's or participant's mobile device without them doing anything active to provide it. This data can include user preferences, configuration information, device usage (including app and data usage), geolocation data, etc. Informed consent must be obtained when using passive data collection.

5.18. Personally Identifiable Information (PII) – Information that can be used to uniquely identify, contact, or locate a single person or can be combined with other sources to uniquely identify a single individual (may also be known as Personal Data). PII definitions vary by jurisdiction.

5.19. Sensitive Information

"Personal Data" is information that relates to an identifiable living natural person. The person may be identifiable from the information in itself, or in combination with other information in the possession of the data controller.

"Sensitive Personal Data" is a specific class of information that may be specifically defined in some jurisdictions such as Europe or Australia. In such jurisdictions, "Sensitive Personal Data" may include information such as racial or ethnic origin, political opinions, religious beliefs, physical or mental health or condition, sexual orientation, and criminal record.

In this Guideline “Sensitive information” refers to a broader class of personal data that may harm or adversely affect the individual. This may be because the respondent may find it upsetting to be asked to disclose this information or, if improperly disclosed, the information could potentially harm or embarrass the individual. This may include financial information, or information about family or personal relationships.

Personal data collected in a research project must be relevant and not excessive.

5.20. Research – The practice of engaging in market, opinion or social research.

5.21. Research Organization – Any individual, company or other entity (such as a not-for-profit organization or government agency) carrying out, or acting as a consultant on a market, opinion or social research project, including those working in client organizations.

5.22. Respondent or Participant - Person from whom or about whom data are collected.

5.23. SMS -- Short Message Service (SMS) is a text messaging service component of phone, web, or mobile communication systems, using standardized communications protocols that allow the exchange of short text messages between fixed line or mobile phone devices.

5.24. Social Media Data – Data about the interactions among people regarding their creation, sharing and exchanging of information and ideas in virtual communities and networks**.**

5.25. Survey - A detailed study of a market or geographical area to gather data on attitudes, impressions, opinions, satisfaction level, past or intended consumer behaviors, etc., by polling a section of a population.

5.26. Web Browsing History - Refers to the list of web pages a user has visited recently -- and associated data such as page title and time of visit -- which is recorded by web browser software for a certain period of time.

6. Types of Mobile Research

6.1. Native mobile apps and mobile web apps

When a native mobile app or a mobile web app is used, researchers must obtain consent and offer respondents an easy to use mechanism to provide that consent. Researchers must not:

- install software that modifies the mobile settings beyond what is necessary to conduct research;
- install software that knowingly causes conflicts with the operating system or cause other installed software to behave erratically or in unexpected ways;
- install software that is hidden within other software that may be downloaded or that is difficult to uninstall;
- install software that delivers advertising content, with the exception of software for the purpose of legitimate advertising research;
- install upgrades to software without notifying users and giving the participant the opportunity to opt out;
- install software that inordinately drains battery life;
- install software that causes any costs to the participant that aren't reimbursed by the research organization
- install or utilize geolocation tracking software that would compromise the participant or their personal data;
- create a risk of exposing personal data during data transmission or storage;
- change the nature of any identification and tracking technologies without notifying the user;
- fail to notify the user of privacy practice changes relating to upgrades to the software; or
- collect identifiable data that may be used by the app provider for non-research purposes; or
- extract information from the mobile device or phone unless this information is part of the purpose of the study (and informed consent is obtained).

Researchers must provide applicable clear and easy to understand privacy policy and T&C (Terms & Conditions) documents that are easy to access via the mobile device being used for research participation. In addition, researchers must demonstrate due diligence in ensuring all of the above. In the case of sensitive information (including personal information), this data can only be collected with informed consent and can then only be used in accordance with applicable law, regulation and relevant research association codes.

Finally, researchers must provide easy to access technical support and clearly communicate how that technical support can be obtained.

6.2. Passive Data Collection

Passive data collection refers to research methods that collect data without the traditional use of survey questions. In many cases and in jurisdictions, this data will be considered personal data or personally identifiable information. Sources of passive data include web browsing history, app data, loyalty data, geolocation data, tracking data from cookies, social media data and other data generated by/obtained from mobile devices. Much of this data can be combined with survey data.

As with personal data or personally identifiable, researchers in many jurisdictions will have to set out a clear legal basis for using and processing this data, including its use to target or trigger survey invitations, and obtaining the informed consent of the individuals concerned.

The following principles should be followed for passive data collection:

- Notice: Providing privacy policies and notices that are clear, short, and standardized to enable comprehension and comparison of privacy practices.
- Limited Collection: Limiting the data collected for research or analysis to information needed to provide research or analytics services and if collecting personal data or personally identifiable information, obtaining consent or utilizing de-identification or de-personalization techniques.
- Choice: Providing consumers with the ability to decline to have their mobile devices used to provide research or analytics services.
- Limitation on Collection and Use: Only collecting data for research or analysis purposes.
- Onward Transfer: Requiring that any 3rd parties, including subcontractors, who have access to passive data, enter into an agreement that requires compliance with applicable industry codes, laws, regulation and these guidelines.
- Limited Retention: Setting policies for data retention and deletion of unique device data and publishing those policies in privacy policy and notices.

6.3. Mobile Market, Opinion and Social Research and Social Media

Mobile devices are being increasingly used for the collection and use of social media data. While this presents new opportunities for researchers, it presents new obligations as well; specifically the obligations to protect research participant privacy, handling personal data complying with the service owners' Terms of Use (ToU), and obtaining necessary permission for the reproduction of material subject to copyright.

For more information, please refer to the CASRO Social Media Guidelines and MRS discussion papers on Online Data Collection and Privacy.

6.4. Mobile Market, Opinion and Social Research via Telephone

With the increase in mobile phone penetration, more and more respondents are participating in telephone research via their mobile phone. In this case the following considerations apply:

- Mobile research participants may incur costs as a consequence of participating in research. While specific costs will vary substantially by country and service provider and service plan, they can include standard telephone charges in addition to charges for data downloads, online access, text messaging and roaming charges and standard telephone charges. If possible, the researcher should design the study so that participants do not incur any cost. If this is not possible, the researcher must be prepared to appropriately compensate the respondent. This compensation can take the form of an incentive.

- When the research design involves calling mobile phones, researchers may sometimes contact potential respondents who are engaged in an activity or in a setting not normally encountered in landline-based calling. This might include driving a vehicle, operating machinery, or walking in a public space. In such cases, the interviewer should confirm whether the potential respondent is in a situation where it is legal, safe and convenient for the potential respondent to take the call. If the interviewer does not receive confirmation, then the call should be terminated while allowing the possibility of making further attempts at another time.

  Applicable laws and regulations governing the calling of mobile phones with which researcher organizations must comply with are listed in Appendix 2.

7. Specific Guidance for Mobile Research

7.1. Photographs, Video and Audio

The capabilities that smartphones and other mobile devices have to create, store and transmit photographs, video and audio provides a new set of tools for researchers. Two such examples are the ability to enhance existing ethnography and mystery shopping methods.

In such cases and any other where a digital image that contains an individual's face that is clearly visible so as to permit the individual to be identified, that image is considered personally identifiable data. Accordingly, all photographs, video and audio recordings gathered, processed and stored as part of a research project must be handled as personally identifiable information. They can only be shared with a client or research user if the participant gives his or her permission, and then only to achieve a research purpose. Information that has been suitably anonymized (such as through pixelisation or voice modification technology) so that it is no longer personally identifiable can be shared with a client or research user client.

The guideline recognizes that there may be instances in which individuals other than the research participant are captured in a photograph, video or an audio recording. In such cases, researchers must gain the permission of these individuals if at all possible. While these individuals are not research participants, the researcher has the responsibility to provide the same privacy protections provided to research participants. If permission cannot be obtained, the researcher must appropriately pixelate or anonymize the photograph, video or audio recording.

In addition, researchers must not instruct participants to engage in surveillance of individuals in public places. Participants should be given specific limited tasks (e.g., capturing interactions with friends, or images of objects or displays) that do not involve monitoring a particular area, where personal data would be captured without the consent of the individuals impacted. When recorded observation of a location is undertaken, clear and legible signs indicating that the area is under observation along with the contact details for the researcher or research organization performing the research should be posted. Cameras should be situated so that they monitor only the areas intended for observation.

Researchers must also caution participants against taking photos or recording in places where these activities are not allowed. Such places include government buildings, banks, schools, airport security areas, private spaces or areas where prohibiting the use of cameras are posted. In all cases, researchers should be aware of all applicable local laws and customs and conduct their research appropriately.

Finally, researchers must take special care when photographing or recording children. This must never be done without the permission of the parent or legal guardian. As indicated above, if permission cannot be obtained, images of children must be appropriately pixelated or anonymized.

7.2. Respondent and Research Participant Safety

As indicated in **“6.4. Mobile Market, Opinion and Social Research via Telephone,”** participants may sometimes be contacted when they are engaged in an activity or are in a setting not normally encountered in landline-based calling.

This is also the case with other mobile research activities and might include driving a vehicle, operating machinery, or walking in a public space. Accordingly, the researcher must communicate the risks and request that participants defer participation until such time where they can safely participate.

Applicable laws and regulations governing the use of mobile phones and devices with which research organizations must comply with are listed in Appendix 2.

7.3. Validation of Mobile Respondents

As with other forms of online research, researchers will need to perform appropriate panelist/respondent and data validation. This includes the removal of fraudulent and inattentive respondents. Many of the technologies and techniques applied to other forms of online research apply. These include cookies, de-duplication approaches and device ID.

With mobile market research, validation may now also be performed using geolocation technology or geolocation data. In some jurisdictions, geolocation may be considered personal data. Accordingly, researchers in those jurisdictions will have to set out a clear legal basis for processing and using this data and obtaining the informed consent of the individuals involved.

7.4. Informed Consent and Opt-Out

As mobile research will often collect personally identifiable information, the following conditions must be met:

- Privacy Policy and Terms and Conditions documents must clearly describe the data that will be collected and how it will be used;
- Informed Consent must be obtained from participants and appropriately recorded; and
- Participants must be able to easily opt-out.

Due to the screen constrains of mobile devices, researchers should consider using layered privacy notices. A layered notice usually consists of a short notice plus a longer notice. The short notice contains basic information, such as the identity of the organization and the way the personal data will be used.

It is important that respondents have sufficient information based on this short notice alone to give informed consent. For example, rather focusing on things respondents probably already know, such as the types of data to be provided by the respondent (e.g. name, age, opinions), the short notice should place an emphasis on data, practices and uses which are invisible to them (geo-location, secondary use, data sharing, data retention).

The short notice contains a link to a second longer notice which contains much more detailed information. Regardless of device users should be able to find the information they are looking for without having to scroll through screens designed to be viewed from a desktop.

7.5. Contacting Respondents

Requirements governing the contact of respondents under various industry codes are as follows:

- Under the CASRO Code interviews must take place at a time convenient for respondents.
- The MRS Code of Conduct limits contact to 9am to 9pm Monday to Saturday, 10 am to 9pm Sunday, unless otherwise agreed in advance.
- AMSRS uses the ACMA Research Calls Industry Standard regarding permissible times to call. These are Monday to Friday from 9am to 8:30pm, Saturday and Sunday from 9am to 5pm. Calls are prohibited on National public holidays, unless otherwise agreed in advance. The phone call must also be terminated if the interviewer finds that it is made to a mobile phone in a time zone where the call is outside the allowed calling times.

The purpose of these requirements is to avoid unreasonable intrusion into the private lives of respondents. Accordingly, researchers should contact respondents only at reasonable times, obtain permission to send updates and notifications by email or SMS and other direct message applications. Researchers should not use excessive reminders. Law and regulation regarding email contact, SMS messaging and opt-out requirements must be complied with.

7.6. Scope of Participant Tasks

The researcher should ensure that any task presented to a participant is of an appropriate length and suitable format. This includes optimizing the format across devices and excluding specific devices if the survey is too long or too complex for a particular device. The likely length of the data collection and the likely time commitment from participants must be clearly explained. Participants must not be deliberately misled regarding the likely time commitment. When applicable, it should be made clear that participants can complete the research at a time convenient to them within the schedule dictated by the project field period.

7.7. Respondent Costs

As indicated in **“6.4. Mobile Market, Opinion and Social Research via Telephone,”** research participants may incur costs as a consequence of participating in research. While specific costs will vary substantially by country and service provider and service plan, they can include standard telephone charges in addition to charges for data downloads, online access, text messaging and roaming charges and standard telephone charges. If possible, the researcher should design the study so that participants do not incur any cost or at minimum, the researcher must notify the participant about the cost of any potential data charges (including roaming charges which could impact participants who are traveling) and give the participant an opportunity to opt-out. If this is not possible, the researcher must be prepared to appropriately compensate the respondent. This compensation can take the form of an incentive. Finally, as contacting participants via mobile telephone call or SMS messaging could incur cost for the participant, some jurisdictions may require prior consent.

7.8. User Experience / Design

Respondents should be given the opportunity to give a considered response (e.g. to amend responses where necessary) and use ‘Don’t know’ or ‘Not applicable’ responses where appropriate.

Mobile devices are a different type of platform and as such have unique limitations to the conduct of research. Researchers should make a considered effort to adapt survey design in order to ensure a positive experience for respondents and minimize data collection bias. A clear point of contact should be available to the respondent in case they have questions during their participation in the research.

7.9. Children

Verifiable consent of a parent or responsible adult must be obtained for that child’s participation in mobile research. The definition of a child varies by jurisdiction. For example:

- under 14 in Australia
- under 13 in the United States
- under 16 in the United Kingdom

7.10. Data and Information Security

Mobile research data must be appropriately secured and protected against unauthorized access. This is essential when the data includes personally identifiable information. This includes accepted techniques including firewalls and encryption. These obligations are also incumbent upon any outsourcing partners protected by proper encryption of the online questionnaire connection and data traffic. Researchers must also ensure that any confidential information provided to them by clients or others is protected (e.g. by firewall, encryption, etc.) against unauthorized access.

Researchers must recognize that personal data stored locally on a participant's mobile device may be potentially available to others should the device be stolen or used by another person. Examples include data stored in native apps installed on the device, photographs that may be taken as part of an ethnographic study and SMS or email messages containing photographs or research data. It is essential that participants be made aware of these risks and that researchers implement reliable encryption techniques and provide participants with instructions on how to password-protect their devices and how to delete all personal information at the conclusion of the research.

Researchers must adequately protect personal data collected or stored on websites or servers. Sensitive or valuable information should be protected by reliable encryption techniques. If temporary storage of the personal data collected takes place on a server that is operated by a provider, the researcher must place the provider under the obligation to take the necessary precautions to ensure that third parties cannot access the data on the server or when it's transferred. Temporary storage of the collected data on the server must be terminated at the earliest possible time.

Appendix 1

Key Fundamentals of the AMSRS Code of Professional Behaviour

The AMSRS Code of Professional Behaviour is based on these key fundamentals for market, social and organisational research:

1. Researchers must conform to all relevant state, national and international laws.

2. Researchers must behave ethically and must not do anything which might damage the reputation of market, social and organisational research.

3. Researchers must take special care when carrying out research among children and young people and other vulnerable groups in the community

4. Participants' cooperation is voluntary and must be based on adequate, and not misleading, information about the general purpose and nature of the project when their agreement to participate is being obtained and all such statements must be honoured.

5. The rights of participants as private individuals must be respected by researchers and they must not be harmed or adversely affected as a result of cooperating in a research project.

6. Participants' identifiable research information must not, without their consent, be revealed to anyone not directly involved in the research project and not be used for any non-research activity directed to individual participants.

7. Researchers must ensure that projects and activities are designed, carried out, reported and documented accurately, transparently and objectively.

8. Researchers must conform to accepted principles of fair competition.

Fundamental Concepts of the CASRO Code of Standards and Ethics

1. Confidentiality: Research organizations are responsible for protecting the identity of individual respondents as well as respondent identifiable information.

2. Privacy and Avoidance of Harassment: Research organizations have a responsibility for striking a proper balance between the needs for research in contemporary life and the privacy of individuals who become the respondents.

3. Internet Research: The unique characteristics of Internet research require specific notice that the principle of respondent privacy applies to this technology and data collection methodology. Specific areas of consideration here are informed consent, transparency and data stewardship.

4. Privacy Laws and Regulations: Research organizations must comply with existing state, federal, and international statutes and regulations and laws governing privacy, data security, and the disclosure, receipt and use of personally identifiable information

The Principles of the MRS Code of Conduct:

1. Researchers shall ensure that participation in their activities is based on voluntary informed consent.
2. Researchers shall be straightforward and honest in all their professional and business relationships.
3. Researchers shall be transparent as to the subject and purpose of data collection.
4. Researchers shall respect the confidentiality of information collected in their professional activities.
5. Researchers shall respect the rights and well being of all individuals.
6. Researchers shall ensure that respondents are not harmed or adversely affected by their professional activities.
7. Researchers shall balance the needs of individuals, clients, and their professional activities.
8. Researchers shall exercise independent professional judgment in the design, conduct and reporting of their professional activities.
9. Researchers shall ensure that their professional activities are conducted by persons with appropriate training, qualifications and experience.
10. Researchers shall protect the reputation and integrity of the profession.

Appendix 2 – Legal Requirements

Australia

State Road Laws and Rules Regarding Use of a Mobile Phone While Driving a Vehicle

While the vehicle is moving or stationary (but not parked), the driver may only use a mobile phone to make or receive a call or use the audio playing function if:

- the mobile phone is secured in a fixed mounting; or
- the mobile phone does not require the driver to touch or manipulate the phone in any way.

All other functions including texting, video messaging, online chatting, reading preview messages and emailing are prohibited.

While the vehicle is moving or stationary (but not parked), the driver must not hold a mobile phone in the hand other than to pass the phone to a passenger.

A mobile phone's GPS (or other driver's aid) function may only be used if:

- the phone is secured in a commercially designed and manufactured fixed mounting, and
- the mounting is fixed in a location that will not distract or obscure the drivers view in any way, and
- the use of the driver's aid does not distract from driving or from being in proper control of the vehicle.

Other relevant Australian authorities and legislation:

Australian Communications and Media Authority (ACMA): http://www.acma.gov.au/

Office of the Australian Information Commissioner (OAIC): http://www.oaic.gov.au/

Privacy Act 1988 and the Australian Privacy Principles

Telecommunications Act 1997

United Kingdom

Driving and Mobile Devices

In the UK it is illegal to ride a motorcycle or drive using hand-held phones or similar devices. The rules are the same if a driver is stopped at traffic lights or queuing in traffic. It is also illegal to use a hand-held phone or similar device when supervising a learner driver or rider.

Drivers can use hands-free phones, sat navs and 2-way radios. But if the police think a driver is distracted and not in control of their vehicle they could still get stopped and penalized.

Automated calling systems and Predictive dialers

Sections 128 to 131 of the Communications Act 2003 gave the Office of Communications (Ofcom) powers to take action against persons or companies who persistently misuse electronic communications networks or services in any way that causes or is likely to cause unnecessary annoyance, inconvenience or anxiety.

The Ofcom Statement of Policy on these powers provides a list of examples of 'misuse'. Six examples are given:

- misuse of automatic calling systems;
- misuse by making silent or abandoned calls;
- number-scanning;
- misuse of a calling line identification facility;
- misuse for dishonest gain; and
- misuse of allocated telephone numbers.

An "automatic calling system" makes calls without live speech, and as such includes Interactive Voice Recognition (IVR) systems making out bound calls. While calls other than for the purpose of direct marketing are not specifically prohibited, they may be considered misuse by Ofcom. IVR systems should not be used in the UK without the prior agreement of the individuals being called.

The Statement of Policy also contains number of technical provisions relating to the use of dialers, with the aim of preventing silent or abandoned calls. These are set out in the MRS document, *Regulations for Use of Predictive Diallers:*

http://www.mrs.org.uk/pdf/2012-02-23%20Regulations%20for%20Predictive%20Diallers.pdf

Other UK guidance and legislation to be considered whilst conducting mobile research

Information Commissioner's Office

Personal Information Online Code of Practice

http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/personal_information_online_cop.pdf

Privacy Notices Code of Practice

http://www.ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Detailed_specialist_guides/PRIVACY_NOTICES_COP_FINAL.ashx

This document contains deathbed guidance on the purpose and development of privacy notices as well as how to draft a layered privacy notice.

Guidance on the Rules on Use of Cookies and Similar Technologies

http://www.ico.gov.uk/news/blog/2011/~/media/documents/library/Privacy_and_electronic/Practical_application/guidance_on_the_new_cookies_regulations.ashx

The Privacy and Electronic Communication Regulations 2003 (Amended 2011) require consent for the placing or reading of information (including but not limited to cookies) from a user's device. MRS guidelines on the application of these rules to research is here:

http://www.mrs.org.uk/standards/eprivacy/

United States

TCPA: The primary US federal regulation governing mobile research is the Telephone Consumer Protection Act ("TCPA"). The regulations have been promulgated and are enforced by the Federal Communications Commission and are content and purpose neutral, i.e., they apply to all calls, regardless of whether they are commercial in nature. Under the TCPA, it is illegal for any person to make a call using an automatic telephone dialing system to any cell phone, except with the prior consent of the called party. The sole exclusion that may be applicable to mobile research covers calls made by or on behalf of a mobile carrier to its customers in connection with the provision of mobile services. The TCPA defines automatic telephone dialing equipment as any equipment capable of dialing, storing or generating telephone numbers, even if such capabilities are not used or activated when making the call. Prior consent has been interpreted to mean the explicit, affirmative consent of a mobile telephone owner to receive a call from an autodialer for research purposes. Accordingly, if a consumer lists their cell phone as their preferred contact number, this would not constitute prior consent to receive a research call from an autodialer. The autodialer restrictions of the TCPA apply to text messages as well as voice calls. A number of states have promulgated their own autodialer regulations. For the moist part, however, the federal regulation preempts and supersedes those regulations.

Do Not Call Regulations: The federal Do Not Call regulation has been promulgated and are enforced by the Federal Trade Commission and apply only to commercial telemarketing calls. The FTC has confirmed that the regulation does not apply to calls made for survey research purposes. A number of states have promulgated their own Do Not Call regulations. Most of those retain the distinction established by the federal regulation between telemarketing and informational calls and therefore do not apply to telephonic survey research invitations.

State Driving Regulations: Most states have established regulations prohibiting the use of cell phones for calling or texting except via a hands-free or speakerphone device. Some state courts have held that a remote texter can be held liable to third parties for injuries caused when the distracted driver has an accident. It would be prudent for research organizations calling or texting respondents on their mobile devices to insure that the individuals are not driving or are using an approved hands-free device or speakerphone before continuing with the survey.

Appendix 3 - Contract/Policy Guidance for Subcontractors/Third Party Suppliers of Mobile Research and Related Services

A research provider may use subcontractors or third parties for fulfillment of portions of a mobile research project. When subcontractors are used, CASRO requires that the research provider must check to ensure that they follow appropriate practices and procedures, especially with respect to the privacy and data protection of personally identifiable information. These practices include:

Performance of proper due diligence when identifying and selecting subcontractors;

- Execution of written Non-Disclosure agreements;
- Execution of written contracts that outline duties, obligations, and responsibilities of the subcontractors that address all parts of the research process, especially privacy and data protection; parties involved and address non-disclosure requirements; and
- Engagement in on-going oversight of subcontractors and their activities.

Policies and contracts relating to the research process and privacy and data protection are available from CASRO (http://www.casro.org) through the model documents, agreements, and contracts of the CASRO Privacy Protection Program (CASRO 3P). The CASRO 3P program has been designed to address the needs of various geographies, including the US and the EU.

Model contracts for transfer of personal data from the EU are available from the European Commission (http://ec.europa.eu/justice/policies/privacy/modelcontracts/index_en.htm)