ESOMAR
WORLD RESEARCH

# ESOMAR GUIDELINE FOR CONDUCTING MOBILE MARKET RESEARCH

World Research Codes and Guidelines

ESOMAR
WORLD RESEARCH

All ESOMAR world research codes and guidelines, including the latest updates, are available online at www.esomar.org

# ESOMAR GUIDELINE FOR CONDUCTING MOBILE MARKET RESEARCH

## CONTENTS

# 1. INTRODUCTION

In 2010, ESOMAR in cooperation with CASRO released a first guideline for conducting research via mobile phones. This addressed the legal, ethical and practical considerations for conducting market research by using voice or text messaging (SMS) to contact respondents on their mobile phones. Since then the use of mobile devices of all kinds (feature phones, smartphones, tablets, portable computers and other similar mobile devices) has grown dramatically across the globe and, in the case of smartphones and tablets, has enabled a new range of research methods. These include online surveys, passive data collection, geo-location and geo-fencing applications, open ended mobile contextual data, online diaries and other forms of mobile ethnography where respondents record their and other people's everyday movements, sometimes taking advantage of portable photographic and video technology.

At the same time, mobile marketing applications continue to expand in number and sophistication. These applications also collect large amounts of personal data and it is not always clear to consumers what data are being collected and how those data are used. Terms of use are not always spelled out clearly and, too often, consumers simply ignore them.

The fact that so much personal data can be collected so easily has caused regulators to question whether current legislation provides sufficient guarantees that individuals are aware and informed when personal data are being collected and shared. Areas of special focus are notice, choice and consent, security and accountability.

Therefore, it is critical that ESOMAR expand its earlier guidance to include the conduct of market, social and opinion research using mobile devices. To that end ESOMAR partnered with the Mobile Marketing Research Association to develop this new guidance. Its purpose is to promote respectful relationships with the individuals contacted for research purposes and to assist researchers in addressing legal, ethical, and practical considerations when conducting mobile market research.

## 1.1. Scope

This guideline covers the collection of information by mobile device (mobile phones, tablets and other similar mobile computing devices) for market, opinion or social research purposes (hereafter referred to as market research). It recognises that there are many different activities enabled by these devices of which market research is just one. These may include personal communication and accessing social media networks but also advertising and direct marketing. It is critical that researchers do not allow any personal data they collect in a market research project to be used for any purpose other than market research.

Throughout this document we use the word "must" when describing a principle that researchers are obliged to follow in order to comply with the ICC/ESOMAR Code. The word "should" is used when describing implementation of a principle. This usage is meant to recognise that researchers may choose to implement a principle in different ways depending on the design of their research.

This guideline should be read in conjunction with the ICC/ESOMAR International Code on Market and Social Research and other ESOMAR guidelines listed at the end of this document and available at www.esomar.org.

## 1.2 Definitions

**Consent** means the freely given and informed agreement by a data subject to the collection and processing of their personal data. In market research, this consent is based on the fact that the respondent voluntarily provides answers in a survey having been provided with clear information about the nature of the data being collected, the purpose for which it will be used and the identity of the person or organisation holding the personal data. The respondent may withdraw their consent at any time by refusing to cooperate in an interview or research project.

**Market research**, which includes social and opinion research, is the systematic gathering and interpretation of information about individuals or organisations using the statistical and analytical methods and techniques of the applied social sciences to gain

insight or support decision making. The identity of respondents will not be revealed to the user of the information without explicit consent and no sales approach will be made to them as a direct result of their having provided information.

**Mystery shopping** is a type of observational study where someone is sent into a business location to act in the role of a customer to evaluate the performance of a business or an employee according to a structured protocol.

**Personal data,** sometimes referred to as personally identifiable information (PII) means any information relating to an identified or identifiable natural person, i.e. a private individual as opposed to a corporate or other comparable entity. An identifiable person is someone who can be identified directly or indirectly, in particular by reference to an identification number or the person's physical, physiological, mental, economic, cultural or social characteristics. In some types of research where there may be no data records per se, individuals might also be identifiable because of photographs, video and audio recordings, or other personal information collected during the research.

**Researcher** is defined as any individual or organisation carrying out, or acting as a consultant on, a market research project, including those working in client organisations and any subcontractors used such as technology providers.

**Research user or client** is any individual or organisation that requests, commissions or subscribes to all or any part of a market research project. The research user receives the results of the research but not the personal data, unless informed consent for this has been given by the respondent.

**Sensitive data** means any information about an identifiable individual's racial or ethnic origin, health or sex life, criminal record, political opinions, religious or philosophical beliefs or trade union membership. In some countries income or other financial information, financial identifiers and government-issued or financial identity documents may also regarded as sensitive.

## 2. KEY PRINCIPLES

All of the core fundamental principles of the ICC/ESOMAR International Code apply to mobile market research. This section describes the how these principles should be operationalised in that context.

### 2.1 Distinguishing market, social and opinion research as the purpose

Researchers must not allow any personal data they collect in a market research project to be used for any other purpose than market research. The ICC/ESOMAR Code requires researchers to be transparent in their dealings with research participants and to not misrepresent as market research any project that has another purpose. To aid clarity and protect the reputation of the researcher and of market research in general, the researcher should present the research services and the organisation or company carrying them out in such a way that they are clearly differentiated from any non-research activities. It is recommended that:

- The organisation's privacy policy, promotional literature and contracts differentiate the different services offered and separate market research from other activities;
- it is easy for participants and others to contact the researchers carrying out market research and those making enquiries without being confused by having to deal with a non-research organisation or deal with non-research staff to raise queries or complaints about market research activities; and
- the introduction used when contacting a potential research participant must clearly define the purpose so that a potential participant is not left with the impression that the exercise has a research purpose if it does not.

These requirements do not prevent researchers from being involved in non-research activities providing the purpose of collecting personally identifiable data is not misrepresented and that any personally identifiable data are not used for another purpose unless specific informed consent is obtained from each participant. Nor do they in any way restrict the right of the organisation to

promote the fact that it carries out both market research and other activities providing they are clearly differentiated and that they are conducted separately and in accordance with the relevant laws and local professional rules of conduct.

## 2.2 Conforming to the law

Mobile technology and communications have grown rapidly in some countries and at a slower pace in others, and legal frameworks are still evolving. Only a few countries have addressed the legal parameters for unsolicited communication and interaction with mobile device users. The regulatory dimension is complicated by the multiple communication mediums that mobile devices provide. Further, there may be national laws that pertain specifically to mobile users, e.g., restrictions on using mobile phones while driving. Such regulations indirectly affect, and could potentially be construed as establishing legal liability for a researcher contacting a potential research participant via a mobile device.

Given the above it is critical that researchers be aware of and respect regional, national and local laws and regulations as well as relevant cultural dispositions that may mandate a stricter standard of practice than described in this guideline. In some countries anti-spamming laws prohibit unsolicited approaches or messages to potential participants by text or other electronic means such as email. Even where such laws do not exist Internet service providers (ISPs) or mobile service providers may have their own policies to protect customers from unwanted contacts.

In all cases, researchers must remain mindful of concerns about privacy and intrusion and not make unsolicited email approaches to potential participants even in countries where this is still permitted by the law unless individuals have a reasonable expectation that they may be contacted for research due to a pre-existing relationship with a company or organization. Researchers should also reduce any inconvenience such an email might cause to the recipient by clearly stating its purpose in the subject heading and keeping the total message as brief as possible. The same requirement applies to other electronic messages (e.g., instant messaging and SMS).

In the case of calling mobile phones researchers should recognise that even where legislation restricts unsolicited calls for commercial purposes but not market research, it is important to consult and apply any existing research-specific do-not-contact lists for mobile as well as fixed line phones.

Some countries have laws or standards that specify calling hours allowed for unsolicited calls of any type and these should be observed for surveys via mobile phones as well. Mobile phone numbers rarely indicate the respondent's location and therefore the researcher should anticipate that the person being contacted might be in a different time zone, and thus verify the convenience of the time, location and situation. In the absence of such requirements, researchers should observe the same calling hours as for fixed-line phone surveys. For surveys in the business-to-business sector, acceptable times are implicit in the office hours of the business concerned. Similar attention should be paid to the sending of SMS text messages to mobile phones to avoid the participant receiving the message received alert outside "normal hours".

Researchers should note that a number of countries restrict the use of auto-diallers and other automated dialling equipment including predictive diallers[1]. Some countries[2] may permit the use of such equipment only if a person has given prior explicit consent (for example, as a member of an access panel) to be dialled by automated dialling equipment. Where automated diallers are permitted and used, "abandoned or silent calls", where no live interviewer is immediately available, are not allowed.

[1] This includes Germany and the UK.

[2] This includes the US.

## 2.3 Consent and notification

The ICC/ESOMAR Code states that research participants' co-operation must be based on adequate information about the purpose and nature of the research and their agreement to participate obtained. In some countries, existing data protection laws may also require participants be informed when personal data are to be collected.

Therefore, researchers must always obtain informed consent from each research participant before collecting and processing any form of personal data and be completely transparent about the information they plan to collect, the purpose for which it will be collected, how it will be protected, with whom it might be shared and in what form. The information should be clear, concise and prominent. Participants must never be misled, lied to or tricked. Participation in research is always voluntary and participants must be allowed to withdraw and have their personal data deleted at any time.

If at any time during the research there are material changes in the research plan (for example, additional passive data collection such as location or identifiable data shared with research user clients) participants must be informed prior to implementation so that they can make an informed choice about whether to continue in the research. When research involves multiple waves of data collection or extends for several months or longer, researchers should periodically refresh consent by reminding participants of the data being collected, the reasons for collecting the data and the intended use.

As with other forms of data collection for research purposes, researchers must inform mobile research participants of their privacy policy, explaining how any personal data they collect are handled. The standard elements in the privacy policy should include:

- Identification of the company doing the research, its place of business and other contact information;
- a guarantee of confidentiality;
- a promise to not mislead about the nature of the research or its intended use;
- a reminder that all research is voluntary and participants may withdraw at any time as well as ask that their personal data be deleted or corrected;
- a clear statement about any tracking, cookies or tags or passive data collection that may be used and what data are captured;
- a clear statement about how research with children is carried out;
- a description of where personal data will be held, and how they will be protected.

A more detailed discussion of the necessary elements of a privacy policy can be found in Section 2.3 of *The ESOMAR Guideline for Online Research.* Appendix 2 of that document also contains an example policy.

Where the privacy policy is to be delivered via a mobile device, space limitations on the screen of many mobile devices make it difficult to display a full privacy policy and so researchers should provide a solution that minimises cost while maximising convenience in accessing the relevant information. Strategies may vary but one solution is a layered hypertext document with a concise top level statement on how privacy will be protected and data used, a second level general introduction that describes the purpose and general principles and a third detailed section covering all aspects of how the researcher treats personal data.

Participants must also be informed of the law(s) under which the data are being collected. In the EU, ESOMAR requires the researcher collecting the data (the data controller) to comply with the law of the country where they are established and, if collecting data in several countries, also to comply with the laws of those countries in which research is taking place. Where it is possible to know the participants' country of residence, researchers should follow the legal requirements of that country noting that requirements in the EU are not exactly the same, for example, both Germany and Italy have stricter requirements than other member states. EU law in this area is still being clarified and ESOMAR will monitor developments.

With all of these issues ESOMAR's advice to researchers is to consider the participant's point of view and that, in participating in research, people will assume that the legal requirements of their own country will be met.

## 2.4 Protecting personal data

Data privacy legislation applies only to personally identifiable data, not to data sets where it is impossible to identify any individual. For example, the inclusion in a data set of a name, address, email address or phone number would create personally identifiable data. It might also occur if there were an exact geographic location or postal code that could be combined with other information in the data set.

Researchers must ensure that data sets or other materials (photographs, recordings, paper documents, etc.) collected for market research that contain personally identifiable information are kept securely and are only used for market research purposes. Personally identifiable data can only be passed onto a research user, if the participant has explicitly expressed this wish, or gives explicit consent and on the understanding that no commercial activity will be directed at them as a direct result of their having provided information. Researchers are advised to have written agreements with research user clients to ensure these requirements are respected. Personally identifiable data collected for research purposes cannot be used for non-research purposes. However, data that have been anonymised and therefore no longer personally identifiable can be passed on to research user clients and processed for other purposes.

Researchers should also recognise that some personally identifiable information may be characterised as "sensitive" and therefore handled with greater care.

Two features of newer data collection methods like mobile make protection of personal data more complex: (1) increased involvement of research users in the research process and (2) shortened cycle times. It therefore is essential that researchers anticipate the potential for research users to inadvertently hear or see things that may be defined as personal data and design the research to minimise such risks. Likewise, interim deliverables or sharing of research materials via applications such as online portals should be designed with the same protections as planned for final deliverables.

Data privacy legislation normally specifies an individual's right of access to data held in a personally identifiable form, to view records being held in their name and to request corrections if there are errors. This right of access no longer applies once the data have been anonymised.

Before personal data are transferred from the country of collection to a third country, the researcher must ensure that the data transfer is legal, and that all reasonable steps are taken to ensure adequate security to maintain the data protection rights of individuals. This also applies if using a "remote" server in a different country to collect data from the respondent or if it is processed in an international "cloud". The researcher should explain this process in their privacy policy and provide appropriate safeguards to protect personal data when asking the respondent for permission for the data transfer.

Given the heightened sensitivities concerning personally identifiable data among the general public and regulators, researchers should always use conservative approaches to data release and transfer, bearing in mind their desire to maintain consumer trust and have this recognised by legislators.

## 2.5 Ensuring no harm

Another key principle of the ICC/ESOMAR Code is that the rights of research participants as private individuals must be respected and they must not be harmed or adversely affected as the direct result of participating in market research.

Researchers should recognise that personal data stored locally on a participant's mobile device is potentially available to others should the device be stolen or used by another person. Examples include data stored in data collection apps installed on the device, photographs that may be taken as part of an ethnographic study and messages (by SMS or email) that may have been used to transmit data. It is essential that participants be made aware of these risks and that researchers implement practices to protect personal data such as data encryption, password-protecting the device or providing respondents with instructions on how to delete all personal information at the conclusion of the research.

Unlike most other research methods, mobile research participants may incur costs as a consequence of participating in research. While specific costs will vary substantially by country and service provider, they can include charges for data downloads, online access, text messaging, data plan overages, roaming charges and standard telephone charges. If possible, the researcher should design the study so that participants incur no cost. If this is not possible, the researcher must be prepared to offer compensation. Where mobile participants are added to a panel or sampling database the issue of cost and compensation should be agreed to at the "sign up" stage.

Researchers should also inform participants prior to installing or activating apps that may degrade battery life. The researcher must take all reasonable precautions to ensure that respondents are not harmed as a direct result of participating in research. Some mobile research methods involve asking participants to go to specific places or perform specific tasks. In such instances researchers should caution participants against doing anything that might put them at risk or break the law. Examples include warning participants not to text or otherwise interact with their mobile device while driving or taking photos in places or situations where this is prohibited.

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 fixed-line calling. This might include driving a vehicle, operating machinery, walking in a public space, or when the caller is in another country/time zone. The researcher should confirm whether the potential respondent is in a situation where it is legal, safe and convenient to take the call. If the researcher does not receive confirmation, then the call should be terminated while allowing the possibility of making further attempts at another time. Furthermore, a researcher might contact a potential respondent who is engaged in an activity or in a work or social situation where others may overhear the call and confidentiality is compromised. Since a respondent could be reached in a public or semi-private space, the researcher must consider the nature of the research content in light of the possibility that the respondent might be overheard and personal information or behaviour inadvertently disclosed or responses modified on account of the respondent's situation. If appropriate, the call should be rescheduled to another time or location when confidentiality will not to be compromised.

Finally, researchers must remain mindful of concerns about privacy and intrusion and politely terminate the call if it becomes apparent that the recipient is not in a position or does not wish to take the call, is not competent, or is a child (unless the researcher receives permission from an appropriate adult to proceed with the call). If the respondent is not competent some jurisdictions may require that the researcher offer the opportunity to complete the survey via another method. If the respondent is a child, the researcher must not go further with the interview unless permission is obtained from a parent or legal guardian to invite a child to participate in research.

## 2.6 Children

Researchers must take special care when carrying out research among children and young people. All reasonable measures should be taken to ensure that verifiable and explicit permission is obtained from a parent or legal guardian (hereafter referred to as 'parent') to invite a child to participate in research, or to install an app on their mobile phone, although it is recognised that the identification of children and young people sometimes is not possible with certainty.

Researchers must observe all relevant laws and national codes specifically relating to children and young people noting that the age definition for children varies from country to country. Where there is no specific national definition, those aged under 14 should be treated as "children" and those aged 14-17 as "young people." These age ranges generally recognise the different stages of mental and psychological development.

When first contacting a potential participant whom one might reasonably expect to be a child, researchers must ask for the person's age before any other personal data. If the age given is below the nationally agreed upon definition of a child, the child must not be invited to provide further personal data until the appropriate permission has been obtained. The researcher may ask the child to provide their parent's contact details so that permission can be sought. The request to the parent must include all relevant information about the research as detailed in Section 2.3 above.

Where personal data collected from children will only be used for research purposes and no personal data will be passed on for any other purpose, permission can be a return email from the parent or other suitable method that is in compliance with the relevant laws and national codes.

Prior parental permission is not required to:

- Collect a child's or parent's email address solely to provide notice of data collection and request permission or
- collect a child's age for screening and exclusion purposes. If this screening leads to the decision that a child does qualify for interview, parental permission must then be sought to continue with the interview.

In ensuring that all reasonable precautions are taken to ensure respondents are not adversely affected as a result of participating in a research project, asking children and young people questions on topics generally regarded as sensitive must be avoided wherever possible and in all cases handled with extreme care. Researchers should consult the *ESOMAR Guideline on Interviewing Children and Young People* for more details.

### 2.7 Reputation of the industry

Researchers must not do anything that might damage the reputation of market research. They must always be mindful of the core principles of the ICC/ESOMAR Code in the work they and their companies conduct and avoid activities and practices that could undermine public confidence in market research.

Some people consider their mobile phone to be a personal and private instrument. The researcher must be sensitive to these privacy concerns and therefore differentiate the calling protocols for research via mobile phone from the practices used in fixed-line phones research. For example, the researcher should consider limiting the number and pattern of call-backs when contacting a known mobile number.

In line with the ICC/ESOMAR Code requirement that researchers identify themselves, calls to mobile numbers should be set to allow the display of the caller's number where this is possible and this facility should not be deliberately suppressed. If the researcher chooses to leave a voicemail message for a potential respondent (who may have to pay to retrieve the message) then this message should detail how the researcher will offer to recompense for the cost of retrieval.

Wherever feasible, it should be made possible for the called party to contact the researcher by calling the number displayed to establish the researcher's identity. It is good practice to provide a toll-free contact number, recognising that the respondent may need to call the researcher over a fixed-line.

### 2.8 Reporting

The ICC/ESOMAR Code requires that projects are reported and documented accurately, transparently and objectively. This includes notifying research user clients prior to work commencing if any part of the work is to be subcontracted outside the researcher's own organisation. Research user clients must be told the identity of any such subcontractor on request.

## 3. SPECIAL CONSIDERATIONS FOR MOBILE MARKET RESEARCH

### 3.1 Downloadable and web-based apps

Where researchers install apps on mobile interactive devices or when the research requires the use of web-based apps, they must obtain consent and offer respondents an appropriate channel and mechanism for giving permission and a place where they can read more about the relevant privacy policy. Researchers must also disclose to potential participants the purpose of the app, the specific data it collects or uploads, and any impact it may have on the functioning on other installed apps or the performance of the device in general. To the maximum extent possible researchers should ensure that any app required as part of the research

does not:

- Install software that modifies the mobile settings beyond what is necessary to conduct research and does not cause any conflicts with operating systems 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 advertising testing;
- install upgrades to software without notifying users and giving the participant the opportunity to opt out;
- 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; or
- 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.

Researchers who deploy tracking technologies for research must also be proactive in managing distribution of the software and vigorously monitor their distribution channel and look for signs that suggest unusual events such as high churn rates.

## 3.2 Passive data collection

Passive data collection refers to a family of research methods that acquire personal data from participants without the traditional asking and answering of survey questions. Sources for passive data collection include web browsing data, loyalty cards and store scanners, geo-location data from mobile devices and some types of social media data. As mobile technology continues to evolve many of these data sources can now be accessed via mobile. These developments bring a growing need to differentiate market research from other activities and for transparency with respondents about the information that is being collected, especially in view of data protection legislation.

In many countries, some of these activities are controlled by data privacy legislation[3], but these activities can also raise ethical concerns as well as legislative issues. Researchers must either have the respondent's consent before collecting and processing data from these and similar passive methods or the data must be effectively anonymised noting that consent is needed for sensitive data and for placing apps and similar technology as described above.

While it is possible to passively detect the type of device a participant is using, this is not personal data since the purpose of detecting device type is to optimise app performance and survey rendering (e.g., smart phone versus tablet) as opposed to collecting personal data.

A more detailed discussion may be found in the *ESOMAR Guide on Passive Data Collection, Observation and Recording.*

## 3.3 Photographs, video and audio recordings

The ability of smart phones and other mobile devices to create, store and transmit photographs, video and audio recordings has provided a new set of tools for researchers to integrate into their methodologies. Two prominent examples where these capabilities have enhanced traditional methods are ethnography and mystery shopping.

Researchers must recognize that anytime a digital image contains an individual's face that is clearly visible and allows for that individual to be identified it is considered to be personally identifiable data. Therefore, all photographs, video and audio recordings gathered, processed and stored as part of a research project must be handled as such. They can only be passed to a research

[3] Note, the EU Privacy and Electronic Communications Directive places restrictions on the use of traffic data and location data, and requires users' consent to such passive data collection from their device even where it is not personal data as defined in Europe.

user or client if the participant gives his or her permission and even then only to achieve a research purpose. Information that has been anonymised (such as through pixelisation or voice changing technology) to a point where it is no longer personally identifiable can be passed to a research user client and processed for other purposes.

The guideline recognizes that there may be instances in which someone other than the participant is captured in a photograph or video and it may be impractical or even impossible to gain permission. Examples include store personnel and passing pedestrians. While these individuals are not defined as research participants, the researcher nonetheless has the responsibility to accord them the same respect and privacy protections as research participants.

Some types of observational research may involve photographing, videoing or recording in public settings involving people who have not been recruited as research participants. In such instances researchers must gain permission to share such images from those individuals whose faces are clearly visible and can be identified. If permission cannot be obtained then the individual's image should be pixelated or otherwise anonymised. In addition, clear and legible signs should be placed to indicate that the area is under observation along with contact details for the individual or organisation responsible. Cameras should be sited so that they monitor only the areas intended for observation.

Researchers must also caution participants against taking photos or recording in places where this is not allowed such as government buildings, banks, schools, airport security areas, private spaces or any area where signs are posted prohibiting the use of cameras. In all cases, researchers should be aware of any applicable local laws and customs and conduct their research appropriately. More practical details may be found in the *ESOMAR Guide on Passive Data Collection, Observation and Recording.*

Finally, researchers must take special care when photographing or recording children. It must never be done without the permission of the parent or legal guardian. This requirement carries over to public spaces where researchers should avoid capturing images of children even as passersby or in the background. Should images of children be captured inadvertently, their faces must be masked or pixelated to protect their identity.

As with all personally identifiable data researchers should always use conservative approaches to data release and transfer and are advised to gain agreement from the research user on this matter in advance.

### 3.4 Mystery shopping

Mystery shopping presents a special case because by its very nature research subjects are unaware they are being observed. Researchers carrying out mystery shopping studies must take care to ensure as far as possible that individual privacy is respected and that research subjects are not disadvantaged or harmed in any way as a result of this work. Their personal data must be protected and no photographs or recordings may be shared with the research user client, unless the subject's permission has been obtained.

For a more detailed discussion refer to the *ESOMAR Guideline on Mystery Shopping Studies.*

### 3.5 Incidental data

In this digital age much opportunity exists for personal data records to be created that are incidental outputs from some everyday transaction or activity. A mobile phone will create records not just of who consumers call and who calls them, but also approximately where they have been – which mobile cell areas they have been connected to. All of these data are legitimately collected for specific purposes such as billing consumers accurately or routing calls to them.

Such personal data can be processed for those purposes and analysed for management purposes, although usually these data contain limited sets of variables and often do not allow much by way of general research insights.

They must not be analysed for different purposes, for example analysing frequently called numbers in order to offer personal discounts, or analysing flight destinations of frequent flyers to make special offers to them for flights to those locations.

The research value of these behavioural data can be extracted when it is combined with other data about customer habits, attitudes or characteristics; in other words, when two independent personal data files are combined. (This is frequently referred to as database enhancement.) This is permissible as long as the following criteria are met:

- The enhancement serves a clear research purpose such as increasing the analytical value of the data;
- the research participant is informed and agrees;
- no action (e.g., delivery of marketing messages) is taken against a participant as a result of the enhancement; and
- the enhancement or matching process is designed so that the personal identity of the participant is never disclosed without their consent.

## 3.6 Appropriate design

When conducting research with respondents on mobile devices the researcher should ensure that any task given to the participant (e.g., a survey, a diary or discussion forum) is an appropriate length and presented in a suitable format that is optimised across devices. While the research continues to evolve, current evidence suggests that mobile respondents may expect shorter interactions with researchers than in other modes such as phone surveys or in-person focus groups. Because of the small size of the screen on some mobile devices it is important that any instructions, questions, or forms displayed be clear and concise. Given the nature of mobile technology respondents may be more easily distracted and more likely to lose concentration or the connection interrupted or dropped.

Similar cautions apply when designing surveys to be administered via mobile phone where anecdotal reports indicate greater difficulty keeping respondents online with mobile phones as opposed to fixed-line phones.

## GUIDANCE ON PROFESSIONAL STANDARDS

Maintaining consumer trust is integral to effective market, social and opinion research. ESOMAR through its codes and guidelines promotes the highest ethical and professional standards for researchers around the world.

The ICC/ESOMAR Code on Market and Social Research, which was developed jointly with the International Chamber of Commerce, sets out global fundamentals for self-regulation for researchers. It has been undersigned by all ESOMAR members and adopted or endorsed by more than 60 national market research associations worldwide.

In addition, ESOMAR has issued the following guidelines to provide more detailed advice on how to address the legal, ethical, and practical considerations of conducting specific areas of research available on the ESOMAR website at www.esomar.org.

- Guideline on Guideline on Online research
- Guideline on Social media research
- Guideline on Distinguishing market research from other data collection activities
- Guideline on Passive data collection, observation and recording
- Guideline on Interviewing children and young people
- Guideline on Customer satisfaction studies
- Guideline on Mystery shopping
- Guideline on How to commission research
- ESOMAR/WAPOR Guide to opinion polls

Queries about implementing the Guideline should be sent to the ESOMAR Professional Standards Committee, professional.standards@esomar.org

## PROJECT TEAM

- Reg Baker, Senior Consultant at Market Strategies International, consultant to ESOMAR's Professional Standards Committee and Editor of the text
- Mark Michelson, Executive Director of MMRA
- Siamack Salari, Founder of EverydayLives
- Gloria Park Bartolone, Senior Vice President of Global Fieldwork Operations at Maritz Research
- Andreas Piani, General Manager Europe of Arbitron Mobile
- Betsy Leichliter of Leichliter Associates, LLC
- Adam Phillips, Chair of ESOMAR's Legal and Professional Standards Committees

The project team was also assisted by James Randall, Head of Ipsos MORI Digital, Guy Rolfe, Global Mobile Knowledge Leader, Kantar Operations, Tim Snaith, Chief Research Officer, OnePoint Surveys and AJ Johnson, Director of Innovation Technology at BrainJuicer.

ESOMAR
WORLD RESEARCH

ESOMAR
WORLD RESEARCH

ESOMAR is the world organisation for encouraging, advancing and elevating market research worldwide.

www.esomar.org

World Research Codes and Guidelines