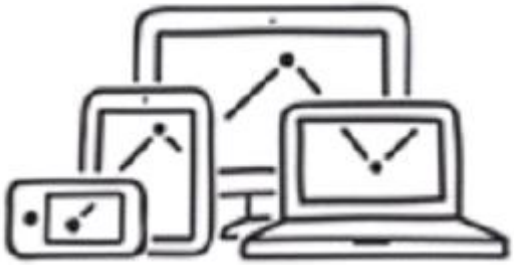
Global Guideline

Mobile Research



ESOMAR
WORLD RESEARCH

GLOBAL RESEARCH
BUSINESS NETWORK
APRC • EFAMRO • ARIA • AMRA

ESOMAR is the global voice of the data, research and insights community, speaking on behalf of over 500 individual professionals and 500 companies who provide or commission data analytics and research in more than 130 countries, all of whom agree to uphold the ICC/ESOMAR International Code**.**

GRBN, the Global Research Business Network, connects 45 research associations and over 3500 research businesses on five continents. www.grbn.org

TABLE OF CONTENT

1 INTRODUCTION AND SCOPE

This ESOMAR/GRBN Guideline on Mobile Research is intended to support researchers, especially those in small and medium-sized research organisations, in addressing legal, ethical and practical considerations when conducting research using mobile devices. It explains how to apply the fundamental principles of market, opinion and social research in the context of the current legal frameworks and regulatory environments around the world. It supplants previous separate guidelines released by ESOMAR and GRBN in 2012 and 2014 respectively. It is a statement of global principles rather than a catalogue of existing regulations.

This Guideline is not intended to substitute for a thorough reading and understanding of the ICC/ESOMAR International Code on Market, Opinion and Social Research and Data Analytics, or the individual codes of the 45 associations that comprise the GRBN. Rather, it is intended to be an interpretation of the foundational principles of those codes in the context of research where individuals share data or information in any setting or in any form that might make it possible to identify an individual.

Finally, this Guideline recognises that technology and governmental regulations continue to evolve, and that there may be different laws and regulations in different countries. And so it seeks to satisfy three key requirements:

1. Be consistent with the spirit and letter of existing laws.
2. Reflect the industry's ethical and professional principles as set out in our professional codes.
3. Be sufficiently broad and flexible to address both current and anticipated future trends in mobile research.

1.1 Scope

This Guideline covers the collection and use of personal data by mobile devices (mobile phones, tablets and other similar mobile computing devices) for the purpose of market, opinion or social research and data analytics (hereafter referred to as 'research'). It also recognises that there are many other activities enabled by these dev ices including general use of the Internet, posting to social media networks, consuming different types of media and online shopping, to name a few. These data, too, may be used for research.

It describes researchers' responsibility when working with both primary data collected for the purpose of research and secondary data that may have been collected for some other purpose but used in research. It describes the practices necessary to comply with relevant industry codes, guidelines and applicable legal requirements in local jurisdictions where research is carried out.

This Guideline also recognises that a range of third parties can be involved as subcontractors in data collection, preparation, analysis, storage, and delivery. These third parties have the same obligations as researchers when personal data is involved.

Many of the practices described in this Guideline - especially those related to consent and privacy protection - are similar to those required for online research. Researchers are strongly urged to consult the ESOMAR/GRBN Online Research Guideline, the ESOMAR/GRBN Guideline on Online Sample Quality and the ESOMAR Data Protection Checklist where many of the requirements and/or recommendations are described in more detail.

Throughout this document the word "must" is used to identify mandatory requirements. We use the word "must" when describing a principle or practice that researchers are obliged to follow. The word "should" is used when describing implementation. This usage is meant to recognise that researchers may choose to implement a principle or practice in different ways depending on the design of their research.

2 DEFINITIONS

For the purpose of this Guideline the following terms have these specific meanings:

Access panel means a database of potential respondents who declare that they will cooperate for future data collection if selected.

Children means individuals for whom permission to participate in research must be obtained from a parent or responsible adult. Definitions of the age of a child vary substantially and are set by national laws and self-regulatory codes. In the absence of a national definition, a child is defined as being 12 and under and a “young person” as aged 13 to 17.

Client means any individual or organisation that requests, commissions or subscribes to a market research project.

Consent means freely given and informed indication of agreement by a person to the collection and processing of his/her personal data.

Data subject means any individual whose personal data is used in research.

Device ID means a distinctive number associated with a mobile phone or similar mobile device. Device IDs are separate from hardware serial numbers. The term “device ID” is often used in research to describe “digital fingerprinting”.

Deductive disclosure means the inference of a data subject’s identify via cross-analysis, small samples or through combination with other data (such as a client’s records or secondary data in the public domain).

Digital fingerprinting means a set of configuration data about a participant's device (such as a computer, mobile phone or tablet) that can be used to create a machine or device fingerprint. Such systems assume the “machine fingerprint” uniquely identifies a device user’s settings and characteristics associated with an individual device or, potentially, an individual user acc bount.

Facial coding means a method of coding the facial muscle movements of an individual to infer emotional reactions in response to various stimuli such as an advertisement or new product concept. This is distinct from facial recognition where the objective is to identify a specific individual in a digital image.

Geolocation means the geographic location of a device such as a computer, mobile phone, tablet, etc.

GPS (global positioning system) means any 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.

Harm means tangible and material harm (such as physical injury or financial loss), intangible or moral harm (such as damage to reputation or goodwill), or excessive intrusion into private life, including unsolicited personally-targeted marketing messages.

IoT (Internet of Things) means the network of physical devices, vehicles, buildings and other items embedded with electronics, software, sensors, actuators and network connectivity that enable these objects to collect and exchange data.

Mobile device means a small, lightweight, hand-held computing device (such as a mobile phone or tablet) typically having a display screen with touch input and/or a miniature keyboard.

Mobile phone (also known as a cellular phone, cell phone and a hand phone) means a device that can make and receive telephone calls over a radio link while moving around a wide geographic area.

Mystery shopping means the use of data collectors trained to observe, experience, and measure a customer service process by acting as a customer or prospective customer and

undertaking a series of pre-determined tasks to assess performance against service quality benchmarks, or to gather information about competitor offerings.

Non-research activity means taking direct action toward an individual whose personal data was collected or analysed with the intent to change the attitudes, opinions or actions of that individual.

Paradata means data about the process by which data was collected, including the behaviour of data subjects during data collection.

Passive data collection means the collection of personal data by observing, measuring or recording an individual's actions or behaviour.

Personal data (sometimes referred to as personally identifiable information or PII) means any information relating to a natural living person (herein referred to as "a data subject") that can be used to identify an individual, for example by reference to direct identifiers (such as a name, specific geographic location, telephone number, picture, sound or video recording) or indirectly by reference to an individual's physical, physiological, mental, economic, cultural or social characteristics**.** Device ID and digital fingerprints are also considered as personal data in some jurisdictions.

Primary data means data collected by a researcher from or about an individual for the purpose of research.

Privacy notice (sometimes referred to as privacy policy) means a published summary of an organisation's privacy practices describing the ways an organisation gathers, uses, discloses and manages an individual's personal data.

Research, which includes all forms of market, opinion and social research and data analytics, is the systematic gathering and interpretation of information about individuals and organisations. It uses the statistical and analytical methods and techniques of the applied social, behavioural and data sciences to generate insights and support decision-making by providers of goods and services, governments, non-profit organisations and the general public.

Researcher means any individual or organisation carrying out or acting as a consultant on research, including those working in client organisations and any subcontractors used.

Secondary data means data collected for another purpose and subsequently used in research.

Sensitive data means any information about an identifiable individual's racial or ethnic origin, health or sex life, criminal record, political opinions, or religious or philosophical beliefs. There may be additional information (e.g. location or financial information) defined as sensitive in different jurisdictions.

SMS (Short Message Service) means a text messaging service component of phone, web or mobile communication system, using standardised communication protocols that allow the exchange of short text messages between fixed line or mobile phone devices.

Social media data means information (e.g. comments or photos) that users generate or share while engaged in or with social media.

Wearables means electronic devices (sensors) that are worn under, with, on top of or as part of clothing capable of collecting and exchanging data without human intervention.

Web browsing history means 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.

3 DATA SUBJECTS: RELATIONSHIPS AND RESPONSIBILITIES

3.1 Ensuring no harm

Researchers must take all reasonable precautions to ensure that data subjects are not harmed as a result of their data being used for research. To that end, they must consider carefully the specific requirements of the research; consult local legal requirements/ restrictions, regulations and customs; and consider practical implications that the research activities may have on data subjects. In all cases, researchers must only ask of data subjects what in the data subject's view is acceptable, safe and fair.

Researchers also must ensure that any software they provide to data subjects is thoroughly tested, complies with the agreed upon privacy protections and does not interfere with or damage the mobile device. See Section 6 - Unacceptable Practices for further details.

3.1.1 Safety

When calling mobile phones researchers may sometimes contact potential data subjects 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 or walking in a public space. The researcher should confirm whether the individual 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.

Some mobile research methods involve asking people to act as data collectors by going to specific places or performing specific tasks. In such instances researchers must caution them against doing anything that might put them at risk, break the law or infringe on the privacy of others. Examples include warning them not to text or otherwise interact with their mobile device while driving or not to take photos or recording in places where this is prohibited (e.g. government buildings, banks, schools, airport security areas, private spaces or areas including shops where notices prohibiting the use of cameras are posted).

3.1.2 Confidentiality and sensitive data

A researcher might contact a potential data subject who is engaged in an activity or situation where others may overhear the call. In this case, the researcher must consider the nature of the research content in light of the possibility that the data subject might be overheard and personal information or behaviour inadvertently disclosed or responses modified as a result of their situation. If appropriate, the call should be rescheduled to another time or location when confidentiality will not to be compromised.

Researchers also must take care when approaching data subjects with topics of a sensitive nature due to the risk of harm or distress. In some countries, authorisation from the relevant national authority to collect sensitive data may be required.

3.1.3 Costs

Unlike most other research methods, data subjects may incur costs as a consequence of participating in mobile research that may include charges for data downloads, online access, text messaging, data plan overages, roaming charges, voicemail message retrieval and standard telephone charges. Researchers should design their research so that data subjects incur no costs without express approval. If this is not possible, researchers must be prepared to offer compensation. Such compensation may be cash, mobile money, airtime or other forms of value.

3.1.4 Distinguishing between research and non-research activities

Researchers must ensure that research purposes are clearly distinguished from non-research activities. In addition, they must not allow any personal data they collect for a research purpose to be used for any other purpose without the data subject's prior consent. This requirement does not prevent researchers from being involved in non-research activities, provided that when collecting personal data for a non-research purpose such

purpose is expressly conveyed to the data subjects, is reasonably differentiated from any research activities involving them and consent for the use of the data for the non-research purpose is obtained prior to data collection.

3.2 Children and other vulnerable individuals

When doing research with children or other vulnerable individuals researchers must consult national laws and self-regulatory codes in the jurisdictions where the data will be collected to determine when parental permission is required or where cultural sensitivities require particular treatment. If when contacting potential data subjects by telephone it is apparent that the data subject is a child, the researcher must not go further with the interview unless permission is obtained from a parent or responsible adult to invite the child to participate in research. If the individual is not competent, some jurisdictions may require that the researcher offer the opportunity to participate in the research using another method.

Researchers must take special care when photographing or recording children. If permission cannot be obtained, images of children must be pixelated or deleted.

Most mobile operating systems have features making it possible, if enabled, to request prior parental consent before installing an app. Researchers should use these settings when developing or commissioning development of an app that is used for research.

3.3 Notification, honesty, consent and the voluntary nature of research

Researchers must obtain consent from data subjects before collecting any form of personal data and be completely transparent about:

- their identity;
- the information they plan to collect;
- the general purpose for which it will be collected;
- the method of data collection;
- how long the data subject is expected to participate;
- how the data will be protected; and
- with whom the data might be shared and in what form.

This information should be clear, concise and prominent. See also section 3.7.1 Privacy Notices. Further, should any of the above information change, further consent by the data subjects is required. Data subjects must never be misled, lied to, tricked or coerced. Participation in research is always voluntary and data subjects must be allowed to withdraw and have their personal data deleted at any time.

Finally, researchers must comply with all relevant laws, regulations and local professional rules of conduct.

3.3.1 Data minimisation and reasonable burden

Researchers must limit the collection and/or processing of personal data to those items that are relevant to the research. They also should ensure that any task given to a data subject (e.g. a survey, a diary or discussion forum) is presented in a suitable format for a mobile device and an appropriate length.

The smaller screen size on some mobile devices means that particular care must be taken to ensure that instructions, questions or forms are clear, readable and concise. This includes optimising the format across devices and excluding specific devices if the survey is too long or too complex for that device. These practices are often referred to with terms such as “mobile first”, “device agnostic” and “responsive design”.

While research continues to evolve, current evidence suggests that mobile data subjects expect shorter interactions with researchers than in other modes such as phone surveys or in-person focus groups.

Similar cautions apply when designing surveys to be interviewer administered via mobile phone where research has shown greater difficulty keeping data subjects online than with fixed-line phones.

3.3.2 Contacting potential data subjects

Mobile technology and communications have grown rapidly and legal frameworks are still evolving. Such regulations indirectly affect, and could potentially be construed as establishing legal liability for a researcher when contacting a potential data subject via a mobile device whether by telephone, email or text messages. For example, in some countries using automated systems to send text messages is prohibited unless explicit consent is obtained.

Researchers must not use any subterfuge in obtaining email addresses or mobile phone numbers of potential data subjects. This includes the use of public websites, the use of technologies or techniques without individuals' awareness or collecting personal data under the guise of some activity other than research. Finally, calls to mobile numbers should be set to display the caller's number; this facility should not be deliberately suppressed.

Researchers must verify with the sample provider (whether a sample supplier or a client) that samples contain only individuals who have a reasonable expectation that they will receive email or text messages soliciting their participation in research.[1]

A full discussion of acceptable practices may be found Section 3.5 of the ESOMAR/GRBN Online Research Guideline.

3.3.3 Telephone research

When calling mobile phones researchers must recognise that even where legislation restricts unsolicited calls for commercial purposes but not research, it is vital to consult and apply any existing research-specific do-not-contact lists for mobile as well as fixed line phones.

Some countries also 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. Researchers 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 telephone research. For research 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 text messages to mobiles to avoid the participant receiving the message received alert outside "normal hours".

Some countries restrict the use of auto-diallers and other automated dialling equipment including predictive diallers. Others permit the use of such equipment only if a data subject 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.

3.3.4 Incentives

Where incentives are offered to encourage participation in mobile research, researchers must ensure that data subjects are clearly informed about:

- what the incentives will be;
- who will administer them;

[1] Other messaging technologies such as mobile application notifications can have characteristics and capabilities that are similar to text messages.

- when data subjects will receive them; and
- whether conditions are attached (e.g. completion of a specific task, access to passive research data, passing of quality control checks, minimum time required as an active member of a community and so forth).

Researchers should carefully consider the use of client-supplied incentives (such as client products or items with client logos) as these may be considered marketing in some jurisdictions.

For a full discussion of incentives, including the use of sweepstakes and free prize draws, see Section 3.6 of the ESOMAR/GRBN Online Research Guideline.

3.4 Passive data collection

Mobile applications are capable of collecting a broad range of personal data without direct interaction with data subjects. Examples include web use and browsing history, app usage statistics, loyalty card data, geolocation, social media data, data from wearables and IoT and other data generated by or obtained from mobile devices.[2]

In addition, specific technologies such as online tracking have valid application in research as a form of passive data collection that typically includes:

- improving the integrity of online samples;
- fraud prevention; or
- research applications, including, but not limited to, online audience measurement, content measurement and advertising testing.

Under these and similar circumstances researchers must make all reasonable efforts to gain consent as described in Section 3.3. Where it is not possible to obtain consent (such as when measuring traffic to a website), researchers must have legally permissible grounds to collect the data and they must remove or obscure any identifying characteristics as soon as operationally possible (see Section 3.7.2 De-identification of data).

3.4.1 Biometric data

Collection of passive and behavioural data also can involve direct interactions with data subjects. For example, facial coding involves recording a data subject's face as he or she completes a survey or similar task. Eye tracking, virtual reality headsets and other wearable devices may be used in a similar way. All of these can involve collection of personal data and, in some cases, data that may be categorised as sensitive in some jurisdictions requiring processes to check compliance with applicable local laws and industry codes.

3.4.2 Photographs and recordings

Photographs, video and audio recordings are considered to be personal data and therefore must be gathered, processed and stored as such. They can only be shared with a client if the data subject gives his or her prior consent with knowledge of the specific purpose for which it will be used. When potentially identifying information has been removed (such as through pixelisation or voice modification technology) so that it is no longer considered personal data it can be shared with a client provided the client agrees to make no attempt to identify the individual.

Researchers must not instruct data subjects (or those that may be acting as data collectors) to engage in surveillance of individuals or public places. Data subjects should be given specific limited tasks (e.g. capturing interactions with friends with their consent, 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 present. When recorded

[2] While it is possible to passively detect the type of device a data subject is using, this is not personal data as long as the purpose is to optimise app performance and survey rendering.

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 organisation performing the research should be posted and images of individuals must be pixelated or deleted as soon as possible. Cameras should be situated so that they monitor only the areas intended for observation.

3.4.3 In-store tracking

In-store tracking of data subjects is a form of passive data collection where the movement of individuals through a store is recorded as they shop. Specific applications fall into two broad categories.

In the first category data subjects are asked to carry a device or download an app that syncs with hardware (such as a beacon) to track and record movement through the store. With this approach standard requirements of notification and consent apply (see Section 3.3 - Notification, honesty, consent and the voluntary nature of research).

In the second category data subjects might not have been told explicitly that they are being observed and behavioural data is being collected while they are in the store. In such cases researchers must ensure that:

- the monitoring and collection of data is permitted by local law;
- there is clear signage to indicate that behaviour is being recorded; and
- any identifying characteristics are removed or obscured as soon as operationally possible.

3.5 Mystery shopping

Data subjects (usually employees) in mystery shopping studies typically are unaware they are being observed. Researchers must take care to ensure that individual privacy is respected and that data subjects are not disadvantaged or harmed in any way as a result of their being the subject of a mystery shopping exercise. Their personal data must be protected and no photographs or recordings may be shared with the client unless permission to do so has been obtained from data subjects, generally as part of an employment contract.

Mystery shopping is distinct from in-the-moment data collection designed to capture a data subject's reaction to the features of the shopping experience and their influence on purchase decisions which is a form of ethnography conducted with consent.

3.6 Use of secondary data

In this digital age an increasing amount of data is created as incidental output from everyday transactions and activities. For example, mobile service providers often collect extensive information about their customers and their use of mobile devices. Mobile phones create records not just of who users call and who calls them, but also geolocation data of where they have been, websites they have visited, which mobile cell towers they have been connected to and so on. They also may record information about the use of individual apps and even data such as posts to social media networks.

These and other similar data present new opportunities for researchers to enlarge their understanding of people's behaviour. While researchers sometimes design projects to collect some of these types of data using traditional methods, much of it may already exist as secondary data that may be available for reuse.

Before using these data, researchers must first ensure that:

- their planned use is legally permissible under the terms agreed to with data subjects prior to data collection and is not specifically excluded in the privacy notice provided at the time of original collection;
- the data was not collected in violation of restrictions imposed by law, through deception or in ways that were not apparent to or reasonably discernible and anticipated by the data subject;

- data subjects had a reasonable expectation that the data might be used for some other purpose, such as research;
- any requests from data subjects that their data not be used for other purposes are honoured; and
- the organisation providing the data has the legal right to share it.

Researchers also must consider whether further processing of the data might risk causing harm to data subjects through deductive disclosure. If such risks exist, researchers must put safeguards in place to mitigate the risk of such harm. This includes but is not limited to ensuring that the identify of individual data subjects is not disclosed or revealed without prior consent and no non-research activity will be directed at them as a direct consequence of their data having been used for research.

3.7 Data protection and privacy

Researchers must adhere to universal data protection principles[3] for personal data. These principles state that any personal data collected or used must be:

- collected for a specified purpose and not used in any manner incompatible with that purpose;
- adequate, relevant and not excessive in relation to the purpose for which it was collected and/or further processed;
- not collected in violation of restrictions imposed by law, through deception or in ways that were not apparent to or reasonably discernible and anticipated by the data subject;
- not used in ways that are likely to result in harm to data subjects, including putting measures in place to guard against such harm;
- protected against risks such as loss, unauthorised access, destruction, use, manipulation or disclosure; and
- preserved no longer than is required for the purpose for which the information was collected or further processed.

There are various standards and frameworks for researchers to use in developing the necessary data security standards and policies. For more information researchers can consult ISO 27001: Information technology - Security techniques - Information security management systems - Requirements or the ESOMAR Data Protection Checklist.

Researchers must carefully consider any decision to store personal data in the cloud. They must assess the cloud storage service provider's security controls and its standard terms and conditions, and be prepared to implement compensating controls when the provider's controls are not sufficient. For further details consult Section 7.7 of the ESOMAR/GRBN Online Research Guideline, the ESOMAR Data Protection Checklist, and The Practical Guide to Cloud Computing.

3.7.1 Privacy notices

Privacy laws and regulations typically require that research companies provide a privacy notice to data subjects. Due to the constraints of screen size of mobile devices researchers should consider using layered privacy notices. This usually consists of a short notice containing basic information, such as the identity of the organisation and the way the personal data will be used plus a longer notice.

Data subjects must have sufficient information based on the short notice alone to indicate their consent and it should highlight data practices and uses that may not be obvious such as

[3] See for example the OECD Privacy Principles.

sound and images, geo-location, secondary use, data sharing, data retention, rather than the obvious types of data collected such as name, age and opinions.

The short notice should contain a link to a second more detailed description and all information should be easily visible without having to scroll through screens designed to be viewed from a desktop.

The privacy notice must state under which law(s) the data are being collected. If collecting data in several countries, the researcher must comply with the laws of the countries where the research is taking place. Where it is possible to know the data subjects' country of residence, researchers must follow the legal requirements of that country noting that there can be considerable variation across jurisdictions.

3.7.2 De-identification of data

Researchers must ensure that any data shared with clients or other data users is sufficiently de-identified to guard against disclosure of personal data. A variety of de-identification techniques exist, each providing varying levels of protection against disclosure of personal data and/or additional security measures. They cover a broad range of data manipulations that include removal of direct identifiers, removal of indirect identifiers (items potentially subject to deductive disclosure) and data transformations (e.g. hashing, encryption, aggregation).

Pseudonymisation is an especially popular technique for de-identifying data during processing and when it may be necessary to recreate the original data for purposes such as matching or validation. It typically involves the separation of personal data from research data, maintaining different IDs in each file and creating a third file linking the two IDs that can be used to reconstruct the original data when needed. Access to the linkage file is limited to only a few individuals. Researchers are strongly encouraged to pseudonymise data as soon as possible after acquisition.

Anonymisation involves a variety of other techniques in which personal data is either deleted or modified so that re-identification of individual data subjects is no longer possible, even by means of deductive disclosure. Examples include removing or encrypting individual data items, blurring images to disguise faces in photographs and videos, introducing noise and only reporting results as aggregated statistics.

3.7.3 Device security

Personal data stored locally on a data subject's mobile device is potentially available to others should the device be stolen or used by another person. Examples include data stored in research or non-research data collection apps installed on the device; photographs taken during in-context ethnographic or other research activities; and SMS, email or other messaging that may have been used to transmit research data that includes personal data.

When collecting data from wearables and other IoT devices, researchers must ensure that all data is encrypted before being transferred across devices.

Data subjects must be made aware of these risks and researchers must implement practices to protect personal data. Examples include data encryption (including encryption of data at rest and data in transit), password-protecting the device, providing data subjects with instructions on how to delete all personal information at the conclusion of the research or other safeguards or controls.

3.7.4 Use of static and dynamic IDs

Research clients and sample providers sometimes use static data subject identifiers (static IDs) to aid in the control and allocation of data subjects within both ad hoc and longitudinal studies. This technique has helped to consolidate information about each data subject and become a useful approach to ensuring unique data subjects within a single longitudinal study and/or adherence to research study exclusion periods.

Some sample suppliers prefer dynamic IDs (variable IDs for every use) to safeguard the identity of individual data subjects.

Researchers should carefully consider the use of each type of ID, balancing data subject privacy and research quality concerns in the context of their specific study.

3.7.5 Use and controls on paradata

Researchers must only use paradata when there is a mutual legal agreement between sample supplier and client to guide, limit and protect the collection, use and onward transfer of these data about the data collection process in the subsequent research and analysis process. In some jurisdictions paradata is considered to be sensitive data.

3.7.6 Transborder transfers

Before personal data are transferred from the country of collection to another country, the researcher must ensure that the data transfer is legal and that all reasonable steps are taken to ensure the privacy and security of these data. This applies if a data collection server is located in a different country from the data subject. It will also apply if cloud technology is used for data storage located in a different country.

The researcher must understand the source and destination countries' applicable privacy laws and regulations governing such transborder transfers, noting that alternative mechanisms for data transfers may exist to facilitate the transfer.

3.7.7 Breach notification

Researchers must comply with all relevant laws and regulations with respect to breach notification and protocol requirements for the country where the data are being collected. Researchers must report security or data breaches first to the relevant authority if such exists, and then to all affected parties including clients, data subjects and subcontractors without unreasonable delay. The notice should include a description of the types of data that were involved in the breach and any steps data subjects should take to protect themselves from potential harm resulting from the breach.

3.8 Sharing personal data with a client

Unless applicable privacy laws and/or regulations stipulate a higher requirement, if researchers plan to collect personal data for research that may also be used for a non-research purpose, this must be made clear to data subjects prior to data collection and their consent for the non-research obtained.

Researchers must not share a data subject's identifiable personal information with a client unless the data subject has given consent to do so and has agreed to the specific purpose for which it will be used.

Even when providing clients with anonymised data sets, researchers must obtain from the client a written guarantee that there will be no attempt to re-identify data subjects unless the above conditions are met.

3.8.1 Observers

Some forms of research include individuals who may have access to personal data by virtue of observing data collection in real time or at some later time via video or a client dashboard. Examples include members of the client team who are not researchers or client subcontractors such as advertising agencies. In such cases researchers must obtain:

- the consent of data subjects to be observed by such individuals (including their affiliations) during or post data collection; and
- formal agreement from all clients and other observers to refrain from disclosing a data subject's personal data or using it in any way other than for a research purpose without consent.

4 CLIENTS: RELATIONSHIPS AND RESPONSIBILITIES

4.1 Subcontracting

Researchers should inform clients, prior to work commencing, when any part of the work is to be subcontracted outside the researcher's own organisation. On request, clients must be told the identity of any such subcontractor.

In cases where the identity of a subcontractor used for sample sourcing can be legitimately considered proprietary information, the sample provider must provide:

- a description of the type of sample sources to be used; and
- an estimate of the percent of the sample expected from panel sources and non-panel sources.

Researchers are also required to ensure that any personal data shared with a subcontractor be limited to what is required to perform the subcontracting task(s); that the subcontractor has the necessary data security procedures in place to protect the data; and that the subcontractor's responsibilities for data protection are clearly documented and agreed to.

4.2 Methodological quality

If users of mobile research are to have confidence that the resulting data are fit for purpose, then researchers must make available appropriate information to clients about how the research was conducted, to enable them to assess the validity of the results including any limitations of the methodology that might lead to conclusions not supported by the data. This information should include:

- sample size, source and management;
- sample design and selection;
- the method of data collection;
- any data cleaning, weighting or post-field adjustments that may have been applied; and
- where mobile penetration is less than 100%, steps taken to ensure that the research results represent the target population of the study.

Specific requirements in each of these areas can be found in the ESOMAR/GRBN Guideline on Online Sample Quality and Section 6 of the ESOMAR/GRBN Online Research Guideline.

4.3 Transparency, misrepresentation and correction of errors

All research projects must be reported on and documented accurately, transparently and objectively. In the event that errors are discovered after delivery, the client must be notified immediately and corrections made promptly.

5 THE GENERAL PUBLIC: RELATIONSHIPS AND RESPONSIBILITIES

5.1 Maintaining public confidence

Researchers must be honest, truthful and objective and ensure that their research is carried out in accordance with appropriate scientific research principles, methods and techniques. Researchers must always behave ethically and must not do anything that might damage the reputation of market, opinion and social research and data analytics. They must always be mindful of the core principles of the ICC/ESOMAR and GRBN Codes in the work they do, avoiding activities and practices that could undermine public confidence.

5.2 Publishing results

See Section 5.2 of the ESOMAR/GRBN Online Research Guideline for a discussion of the researcher's responsibilities when the client intends to publish research results.

6 UNACCEPTABLE PRACTICES

Researchers must not use or install software or applications that:

- have not been thoroughly tested;
- modifies the mobile settings beyond what is necessary to conduct research, without the consent of the data subject;
- causes conflicts with the operating system or causes other installed software to behave erratically or in unexpected ways;
- is hidden within other software that may be downloaded or that is difficult to uninstall;
- delivers advertising content, with the exception of what may be required for legitimate advertising research;
- changes the data collected without notifying the data subject and offering the opportunity to opt-out;
- places unusually high demand on the device's battery unless specific consent is obtained;
- results in costs to the data subject that are incurred without consent and which are not reimbursed by the researcher;
- uses geolocation tracking software without the consent of the data subject;
- transmits personal data that are not encrypted;
- changes the nature of any identification and tracking technologies without notifying and gaining the consent of the data subject;
- fails to notify the data subject of privacy practice changes relating to an upgrade;
- collects personal data that may be used by the app provider for non-research purposes without consent; or
- extracts information from the mobile device or phone unless this information is part of the purpose of the study and consent is obtained.

On completion of the research, any apps no longer required must be deactivated. Data subjects must be notified and given instructions on how to safely remove the app from their device(s).

7 PROJECT TEAM

- Reg Baker, ESOMAR co-chair, Executive Director, MRII and PSC consultant, USA
- Guy Rolfe, GRBN co-chair, Mobile Practice Leader, Innovation & New Technology, Kantar, UK
- Mario Callegaro, Senior Survey Research Scientist, Google, UK
- Simon van Duivenvoorde, Chief Commercial Officer, Wakoopa, NL
- Steve Gutterman, CEO of Mobile Accord, Inc., USA
- Betsy Leichliter, Leichliter Associates, LLC, USA
- Oriol Llaurado, Chief Privacy Officer, Netquest, Spain
- Peter Milla, Consultant to Insights Association, USA
- Paul Quinn, Senior Director, Product Management, Confirmit, UK
- Lisa Salas, Head of Marketing and Operations, TEG Rewards, Australia
- Michael Schlueter, Associate Director Global Innovation, GfK, UK
- Navin Williams, CEO, Mobile Measure, Singapore

ESOMAR: Kathy Joe, Director International Standards and Government Affairs and Jan Willem Knibbe, Policy & Industry Projects Executive