ESOMAR
WORLD RESEARCH

GLOBAL RESEARCH
BUSINESS NETWORK
APRC • EFAMRO • ARIA

Duty of Care: Protecting Data Subjects from Harm

Consultation Draft: August 7, 2019

Table of Contents

1 INTRODUCTION 1

2 PURPOSE AND SCOPE 1

3 DEFINITIONS 2

4 RESEARCH VERSUS NON-RESEARCH ACTIVITIES 3

5 PRIVACY IMPACT ASSESSMENTS 4

5.1 WHAT IS A PIA? 4
5.2 WHAT CIRCUMSTANCES SHOULD TRIGGER A PIA? 5

6 STEPS IN THE PIA PROCESS 5

6.1 CHART THE FLOWS OF INFORMATION THROUGH THE ORGANISATION(S) 5
6.2 IDENTIFY POTENTIAL RISKS AND THEIR SEVERITY 5
6.3 DEVELOP AND EVALUATE SOLUTIONS TO MITIGATE RISKS 6
6.4 SOME SPECIFIC CONCERNS 6
6.4.1 PASSIVE DATA COLLECTION 6
6.4.2 SECONDARY DATA 7
6.4.3 SEGMENTATION VERSUS PROFILING 7
6.4.4 AUTOMATED DECISION-MAKING SYSTEMS 7
6.5 INTEGRATE RISK MITIGATION SOLUTIONS INTO ORGANISATIONAL PROCESSES AND PLANS 8

7 PRIVACY RISKS ASSOCATED WITH SOME SPECIFIC TYPES OF RESEARCH 8

7.1 PUBLIC OPINION POLLING 8
7.2 RESEARCH DATABASE ENRICHMENT AND DATA INTEGRATION 8
7.3 AUDIENCE MEASUREMENT RESEARCH 9
7.4 MYSTERY SHOPPING 9
7.5 SOCIAL MEDIA RESEARCH 9
7.6 ONLINE COMMUNITIES 9
7.7 CUSTOMER EXPERIENCE RESEARCH 9

8 HARMS UNRELATED TO PRIVACY 10

9 REFERENCES 10

10 PROJECT TEAM ..... ERROR! BOOKMARK NOT DEFINED.

1 INTRODUCTION

Decision-makers in all segments of society require a clear understanding of the environment in which they operate if they are to develop products, services, and policies that benefit their varied constituencies. Market, opinion, and social research and data analytics (hereafter "research") provides the data and insights needed for this evidence-based decision-making by commercial organisations, governments, non-profit organisations, and the general public. This often requires the collection and processing of substantial amounts of personal data. In doing so, researchers have a duty of care to those individuals (hereafter "data subjects") whose data we collect and process to protect their personal data and their privacy to ensure that they do not experience adverse consequences or harms as a result of having participated in research.

Historically, researchers' primary ethical responsibility has been to protect data subjects from harms such as unsolicited direct marketing and other similar sales-oriented activities. More recently, the proliferation of data of all kinds and the ability to link data from multiple sources to create rich profiles on individual data subjects has led to new uses of data that go beyond marketing and sales to a host of other domains such as the provision of healthcare services, granting of credit, criminal justice investigations, and employment decisions, to name a few. Such uses not only compromise the privacy of data subjects, they also can be discriminatory, favoring some individuals over others and potentially doing so based on incomplete or biased information.

At the same time, the continually expanding use of modern technologies for data acquisition, processing, analysis and delivery by organisations in all sectors has created a new set of risks for those data subjects about whom these organisations collect, process and store personal data. These risks include the unauthorised release of personal data or data breaches by outside persons or oganizaations.

Meeting our industry's responsibility to protect the privacy and well-being of data subjects requires that organisations that commission or conduct research provide an adequate and effective infrastructure of processes, tools, standards and technologies for protecting any personal data in their possession from accidental or other unauthorized disclosure. Such organisations must recognize that they are ultimately accountable to data subjects and regulators should such disclosures occur.

2 PURPOSE AND SCOPE

The purpose of this document is to advise researchers, the organisations in which they work and those who commission research on their responsibility to protect the privacy and well-being of data subjects who participate in research or whose data is processed for a research purpose. It provides the flexibility for organisations to formulate their own specific solutions to mitigate and address the risks inherent in the types of research they may conduct or commission. It is designed to be especially useful to smaller organisations that might not have extensive resources or experience in information security practices and data protection requirements.

The guideline recognizes that there is considerable variation in regulatory requirements from country to country, with some being more restrictive than others. And so, it takes a global view that emphasizes a researcher's ethical responsibilities independent of the applicable laws in those countries where they collect or process data. Throughout its history the practice of research has been governed by three overriding principles:

1. When collecting personal data from data subjects for the purpose of research, researchers must be transparent about the information they plan to collect, the purpose for which it will be collected, with whom it might be shared, and in what form.

2. Researchers must ensure that personal data used in research is protected from unauthorised access and not disclosed without the consent of data subjects.
3. Researchers must always behave ethically, comply with all applicable laws and regulations, and not do anything that might harm a data subject or damage the reputation of research.

Researchers must adhere to these three principles when undertaking any research activities.

The Organisation for Economic Cooperation and Development (OECD) espouses a similar set of privacy principles that comprise a privacy framework reflected in many existing and emerging privacy and data protection laws worldwide. See OECD Privacy Framework for details.

Finally, this document is not intended to substitute for a thorough reading and understanding of a researcher's responsibilities under the ICC/ESOMAR International Code on Market, Opinion, and Social Research and Data Analytics or the national 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, whether the researcher collects data directly from an individual or accesses data collected by another party for some purpose other than research. Nor does it free researchers or the organization in which they work from their responsibility to be aware of and comply with all national laws, self-regulatory codes, and cultural practices in the jurisdictions where they collect or process data.

3 DEFINITIONS

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

API (application programming interface) means a set of definitions and protocols that can be used to build an application capable of communicating with other applications, often for the purpose of accessing data on a website.

Client means any individual or organisation that requests, commissions, or subscribes to all or any part of a 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 analytics means the process of examining data sets to uncover hidden patterns, unknown correlations, trends, preferences, and other useful information for research purposes.

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

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.

Mystery shopping means the use of fieldworkers, researchers or participants (consumers or general public) in the role of customers/users in order to evaluate a business/service performance.

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.

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 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.

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

Privacy means the ability of a person to control, edit, manage, and delete information about themselves and to decide how and to what extent such information is communicated to others.

Privacy impact assessment (sometimes referred to as PIA or DPIA) means a process to identify and mitigate data subjects' privacy risks.

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

Profiling means the collection and processing of personal data with the intent to analyse or predict a data subject's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements in order to take direct action toward him or her for a non-research purpose.

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 corporations, 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 but subsequently used in research.

Segmentation means an analytic technique aimed at dividing a broad target market into subsets or groups of individuals or organisations who have, or are perceived to have, common needs, interests, and priorities, and then designing and implementing strategies to interact them. Segmentation differs from profiling in that its focus is on well-defined groups of people with shared characteristics rather than individual data subjects.

Sensitive data (sometimes referred to as 'Special Category Data') means specific types of personal data that local laws require be protected at the highest possible level from unauthorized access in order to safeguard the privacy or security of an individual or organisation, and which may require additional explicit permission from the data subject before processing. The designation of sensitive data varies by jurisdiction and can include but is not limited to a data subject's racial or ethnic origin, health records, biometric and genetic data, sexual orientation or sexual habits, criminal records, political opinions, trade association membership, religious or philosophical beliefs, location, financial information, and illegal behaviors such as the use of regulated drugs or alcohol.

Web scraping (sometimes called crawling or spidering) means the use of software to extract large amounts of data from websites.

4 RESEARCH VERSUS NON-RESEARCH ACTIVITIES

Simply put, the essential challenge researchers and those who commission research face is to ensure that data collected and processed for a research purpose is not also used for a non-research purpose without first obtaining the consent of the data subject. This distinction is more than an academic exercise. Many countries recognize the social and economic value of research and their regulatory frameworks allow for more flexibility when the purpose is research. Such as:

- fewer restrictions on unsolicited contacts offering potential data subjects the opportunity to participate in research;
- extended periods of data retention (e.g. archiving);

- less onerous requirements when involving children and young people in research;
- fewer restrictions on the collection and/or use of data that may be defined as "sensitive;" and
- greater freedom to repurpose secondary data for research without requiring consent of the data subjects for such use.

Failure to be truthful and honest in making the distinction between research and non-research activities risks the loss of public confidence and the regulatory benefits that are essential to the long-term sustainability of research as a distinct and separate purpose.

The key distinction between research and non-research is that research limits itself to statistical/social science analysis and the delivery of insights. Researchers have no interest in the identity of individual data subjects except as representatives of a larger group[1]. The identities of those whose personal data is collected and processed are not disclosed and are rigorously protected.

Other activities may be described as research or at least seem similar to research in that people are contacted, questions asked, data recorded, and analyzed. Or, existing data is enriched by harvesting data from other sources and datasets. How the data is used – the purpose for collecting it – determines whether an activity is research or something else. If the purpose is to take direct action toward those individuals whose data is collected or processed, whether to change their opinions, attitudes, or behaviors or impact them in some other personalized way, then the purpose does not qualify as research.

5 PRIVACY IMPACT ASSESSMENTS

As noted at the outset, research typically involves the collection of personal data, either directly from data subjects or indirectly through secondary data sources. In all cases, researchers have a responsibility to ensure that they do not intrude on the privacy of data subjects whose data is collected or processed. A Privacy Impact Assessment (PIA) is a useful tool for an organisation to require of its researchers when designing their research.

5.1 What is a PIA?

A PIA is a risk management tool to identify potential privay risks to data subjects and potential legal compliance risks for the research organisation. Simply put, it is a process to systematically identify and mitigate the risks to data subjects' privacy over a research project's life cycle.

The design of a PIA will vary depending on the organisation's business, its internal processes, and those of any subcontractors used. Assessments should be conducted at the individual project level, occur in the project planning stage, and cover any planned use of personal data. Organisations should retain a record of each assessment, updating it as the project evolves and material changes are made to the original design.[2]

Researchers collecting or processing personal data in countries in the European Union face very specific assessment requirements. Consult (whatever the DPIA document ends up being called) for further details.

---

[1] One exception is the use of personal data for quality assurance.

[2] For an especially useful discussion of PIAs refer to the ICO publication, Conducting Privacy Impact Assessments: Code of Practice.

5.2 What circumstances should trigger a PIA?

Best practice would require a PIA for every project that involves the collection or use of personal data. Where that is not practical, organisations should consder particular project features that signal heightened privacy concerns and therefore require a PIA. For example:

- any data processing on a large-scale, especially with respect to the number of data items, the number of data subjects, the planned retention period, and geographic extent;
- use of datasets that have been matched or combined;
- data collection that involves ongoing and systematic monitoring;
- collection or processing of sensitive data, including special categories of data, but also including financial information or data concerning criminal convictions or offences;
- processing that includes evaluation or scoring, including profiling and predicting;
- processing of personal data by subcontractors;
- use of new technologies or methods;
- collection and processing of data on children or vulnerable individuals; and
- data transfers across borders.

6 Steps in the PIA process

A PIA typically involves these four steps or stages.

6.1 Chart the flows of information through the organisation(s)

Describe in as much detail as possible the purpose(s) for acquiring the data and how it will be collected, processed, protected, and retained. While individual research companies often have similar practices in these areas there also can be considerable variation from organisation to organisation depending on how it is structured, the operations it performs internally as opposed to working through subcontractors, the types of data being processed, and the statistical and analytic techniques used to generate the insights delivered to clients. Pay particular attention to any plans to share data with those outside the organisation (such as subcontractors or clients); uses of data in ways not reasonably anticipated by data subjects at the time of collection; and any planned processing steps that are not necessary to fulfil the purpose(s) of the research.

6.2 Identify potential risks and their severity

At this stage the organisation systematically considers how the project is likely to impact data subjects' privacy. It is equally important at this stage to ensure that the project plan complies with all applicable legal requirements in those countries where data is collected or processed.

While by no means a comprehensive list, there some obvious categories of risk that may arise from research. They include but are not limited to:

- non-research activities, that is, the use of personal data to take direct action toward an individual data subject;
- insufficient differentiation between research and non-research activities, thus exposing data subjects to further direct action taken towards them, including direct marketing;
- collection of excessive or irrelevant information (including sensitive information);
- overly long data retention practices;
- use of data for a purpose not disclosed to data subjects at the time of collection;

- use of data collected by subterfuge or without the knowledge of the data subject;
- disclosure to third parties without consent, including providing personal data back to clients;
- use of data subjects' comments or quotes for advertising purposes; and
- ineffective information security practices that may result in data breaches.

Of these, the first in the list—using personal data to take direct action toward data subjects—has long been a major concern. To address it, researchers have come to rely on a rigorous consent process that, among other conditions, specifies the purpose of the collection, a description of how the data will be used, whether any of it will be shared and, if so, in what form and with whom.

6.3 Develop and evaluate solutions to mitigate risks

This is the point at which the organisation identifies the actions it must take to address the identified privacy risks and ensure compliance with all applicable ethical and legal requirements. The ESOMAR Data Protection Checklist is the recommended resource for solution development. It translates data privacy regulations into everyday terms to guide organisations in meeting their responsibilities within a global data protection framework. It also helps to identify gaps in the organisation's privacy protections.

While it may be fair to describe this step as a cost/benefit analysis, organisations must recognize that failing to meet its obligations to protect the privacy of data subjects can result not just in reputational damage but also in significant fines or litigation. Key to that is ensuring that all staff involved in research projects or handling of personal data regardless of source are aware of and trained in the organisation's privacy protection program.

6.4 Some specific concerns

Throughout much of its history research has relied on primary data collections where privacy guarantees were managed via a rigorous consent process. Over about the last decade the combination of new technologies, a dramatic increase in the amount of data being collected, and increasingly innovative use of that data both for research and non-research purposes has challenged research organisations to rethink their traditional processes for protecting the rights of data subjects. Several specific concerns have emerged and both the research industry and regulatory bodies have begun to work through solutions. The following is by no means an exhaustive list.

6.4.1 Passive data collection

Passive data collection is a widely used research approach and can include but is not limited to online audience measurement, in-store tracking, advertising testing, and attitudes and opinions about brands, products, political candidates, and so on. Common techniques for collection include the use of APIs provided by the website owner and web scraping using third party tools.

When collecting these kinds of data, researchers must make all reasonable efforts to gain consent and limit the use of personal data to research and other legitimate research purposes. Where it is not possible to obtain consent directly form data subjects (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. In addition, prominent information about such data collection and use practices must be made available, even if indirectly, using appropriate platforms to demonstrate efforts are made to compensate for the inability to obtain consent. This could be achieved by participating in recent industry initiatives spearheaded by research industry and professional associations. These can be used to provide indirect and prominent information or opt-out mechanisms geared to data subjects.

Before web scraping is used to collect such data, researchers must consult the Terms of Use for the site as these often prohibit scraping.

6.4.2 Secondary data

Researchers and non-researchers alike increasingly look to acquire and use existing data (both public and privately-held) to augment or replace primary data collection. As in the case of primary data collection, the purpose for which the data is to be used determines the distinction between research and non-research. Thus, researchers must ensure that their planned research use is compatible with the purpose for which the data was originally collected. They must verify or seek appropriate assurances that the original collection was legal and with the consent of the data subjects.

Researchers also must design their research so that further processing of the data does not risk the privacy of data subjects either directly or through deductive disclosure. Organizations must put safeguards in place to mitigate the risk of such harm such as ensuring that the identify of individual data subjects is not disclosed or revealed (either directly or through combining with other data) without prior consent, use measures to reduce the granularity of the data and lower the probability of a data subject being identified, and ensuring no non-research activity will be directed at them as a direct consequence of their data having been used for research.

Consult the *ESOMAR/GRBN Guideline on Secondary Research* for further details.

6.4.3 Segmentation versus profiling

In many cases, the distinction in how personal data may be used in research versus non-research can be expressed as the difference between segmentation and profiling. Segmentation is an analytic technique that identifies a cluster of characteristics that can be used to define groups of people with common needs, interests, and priorities. Its focus is on well-defined groups of people with shared characteristics rather than individual data subjects. Most importantly, the personal data of those data subjects is not shared with clients, even when the sample used in the study may have been provided by the client. Thus, segmentation is a legitimate research activity.

Profiling (sometimes called behavioral targeting)**,** on the other hand, focuses on the collection of personal data about individual data subjects with the intent to use that data to take direct, tailored action toward them as individuals for a non-research purpose such as direct marketing. A common use is in the context of automated decision making systems (See next section). The data may be used in research, but such research is not the primary purpose. The primary purpose is to use personal data to target individuals for a non-research purpose. Therefore, profiling is not research.

6.4.4 Automated decision-making systems

Over the last decade with the explosion of digital data of all kinds, new services have emerged that gather and analyse consumer data for a broad range of purposes, some for research, but most not. Chief among them is the development of automated decision-making systems, that is, rules-based systems that use profiles of individual data subjects to make management decisions. Those decisions cover a wide range of activities with varying levels of impact on the privacy and well-being of individual data subjects, some of which are clearly discriminatory. They may be grouped into four broad categories:

- Loss of opportunity (e.g., in employment, access to insurance and other benefits, housing, and education);
- Economic loss (e.g., granting of credit, pricing of goods and services, narrowing of choice);
- Social detriment (e.g., emotion duress, public embarrassment, selective advertising); and

- Loss of liberty (e.g. increased surveillance, incarceration).[3]

As a result, research has been drawn into a broader discussion about the collection, use, and processing of personal data, especially when using online methods to collect behavioral data, whether by active or passive means. Some organisations now use the term "research" to describe a data-driven industry that profiles individuals not just for marketing and sales purpose, but to automate a broad set of decisions that can affect financial well-being, health, employment opportunities, and so on. This blurring of the lines highlights the difficulty researchers face in continually demonstrating the distinction between market, opinion, and social research and data analytics on the one hand, and non-research activities on the other. Organisations must take care to maintain this distinction in their practice.

Regulatory frameworks across jurisdictions may specify how this data can be used, often in terms of the severity of impacts on individual data subjects. However, organisations must not allow the personal data they collect or process to be used for any purpose that directly impacts an individual subject.

6.5 Integrate risk mitigation solutions into organisational processes and plans

The last step is to implement mitigation solutions identified by the assessment. Each solution should be evaluated in the context of the structure of the organisation and the type of work it performs to determine whether it should be implemented for this specific project or become part of the organisation's infrastructure for all of its research activities. As noted above, the ESOMAR Data Protection Checklist is the recommended resource.

7 PRIVACY RISKS ASSOCATED WITH SOME SPECIFIC TYPES OF RESEARCH

Organisations must ensure that their employees are able to distinguish between valid research practices and other data collection and processing activities that have a non-research purpose, including taking direct action toward individual data subjects.

7.1 Public opinion polling

Public opinion polls are conducted to understand opinion about elections and other political topics at a given point in time. They report on a representative sample of the overall public or some particular sub-group.

However, efforts to sell products, raise funds, or promote a candidate or issue are sometimes disguised as public opinion polls. Participants are asked what appear to be legitimate survey questions, and they are asked to contribute money, buy a product, or add their names to a political mailing list. "Sugging" (sales under the guise of research), "frugging" (fundraising under the guise of research), and campaigning under the guise of research are not research.

7.2 Research database enrichment and data integration

Client organisations sometimes seek to enrich their customer databases with personal data gathered during a research exercise where the primary purpose is research, creating a broader basis for further research. This is legitimate research if the sole purpose is to expand the database for analytic purposes.

However, if the goal is to use the data to take direct action toward individual data subjects it is not research.

---

[3] For further discussion see Future of Privacy Forum (2017), "Unfairness by Algorithm: Distilling the Harms of Automated Decision-Making."

7.3 Audience measurement research

Audience measurement research provides clients with aggregated statistics on the size of the audience that has been exposed to a piece of media content including advertising. This enables a media owner or advertiser to determine the value of any advertising space and is a fundamental function underpinning the provision of a wide range of services and information, particularly radio, TV and the internet.

However, if the segments reported are so detailed and granular that it is possible to target a specific data subject with content tailored to his or her individual requirements, this is profiling and therefore not research.

7.4 Mystery shopping

Mystery shopping helps client organisations to determine whether the promises they make to their customers every day through advertising, branding and the launch of products and services are actually fulfilled at the point of delivery to customers. Examples of the promises may be specific prices and promotions, knowledgeable and helpful staff, clean and welcoming stores, fast telephone service and easy or intuitive online shopping. These promises are supposed to be delivered by front-line staff in physical locations, call centres and chat lines. Mystery shopping measures compliance to the promises given to customers.

Two very different types of studies may be carried out under the general heading of mystery shopping. In the first type, all personal data collected is kept confidential, not shared with the client, and used only for research purposes. In the second, personal data is not treated as confidential and is used by the client to approach data subjects individually for purposes other than scientific research (e.g. individual performance improvement or operation of a bonus system). This latter case where personal data is used for purposes other than research does not qualify as research.

7.5 Social media research

The largely unfiltered postings of social media users are an increasingly fruitful source of insight about a wide variety of issues of interest to companies and organisations across sectors, be they public or private. Understanding social drivers and trends at an early stage allows stakeholders to take early and timely actions.

However, much of that data is personal data in that it can be used to identify data subjects either directly or indirectly, and therefore can be used for non-research purposes. If the intent is to identify individual data subjects so that commercial messages can be targeted at them, or to quote an individual post for promotional purposes, this is not research.

7.6 Online communities

Online communities are an increasingly popular method that allows brands continually to interact with groups of customers and other stakeholders across a variety of topics and thus further new product design, new services, advertising, and satisfaction over an extended period.

While many online communities are research focused, communities also can be used to purposively create brand advocates, that is, brand ambassadors who promote brands to their peers. Brand advocacy communities are normally much bigger than those for research alone and participation is intended to lead to panel members taking an action to promote the brand. Thus, advocacy panels are not research.

7.7 Customer experience research

Customer experience research aims at the collection and analysis of representative sample data to understand the dynamics of satisfaction and retention for a brand/product or experience. The widespread emergence of customer experience research has resulted in new challenges in

maintaining the distinction between research and non-research activities. It is increasingly common for these projects to have two purposes:

1. The collection and analysis of representative sample data to understand the dynamics of satisfaction and retention.
2. Provision to the client of personal data for follow-up with service recovery, sales promotions, or product offerings.

The first instance has a clear research purpose while the second does not. Potential exceptions include instances where the health or safety of the data subject may be at risk or other circumstances as required by law. Researchers must consult local laws and regulatory codes for specific requirements in all jurisdictions where they plan to collect and/or process data.

8 HARMS UNRELATED TO PRIVACY

Finally, there are risks to the well-being of data subjects that are not privacy related, but still must be considered in the project planning stage.

- **Personal injury** that might incur because of participating in research. For example, when conducting telephone studies interviewers may contact a potential data subject who is engaged in an activity or in a setting (driving a vehicle, operating machinery, or walking in a public space) where participating might expose that individual to physical harm. A second example involves product testing where data subjects might be exposed to products that cause them physical harm, including use of tobacco or alcohol products.
- **Legal jeopardy** when data subjects act as data collectors by going to specific places or performing specific tasks. Examples include taking photos or making recordings in places where this may be prohibited (government buildings, banks, schools, airport security areas, private spaces or areas including shops where notices prohibiting the use of cameras are posted).
- **Financial loss** caused by participating in research. Examples include transportation costs to and from central interviewing locations or additional mobile phone charges for texting or data downloads in mobile studies.

Here again, organisations must ensure that their employees are aware of these risks and that their research projects are designed to protect against them.

9 REFERENCES