

# Research

Australian Market & Social Research Society | Volume 32 | Number 3 | April 2015

## News

PRIVACY

10

### LEARNING FROM HACKS

*Silver lining to data breach cloud.*

12

### THE CREEPY SIDE OF PRIVACY

*And then it gets worse.*

14

### A PRINCIPLES-BASED APPROACH TO PRIVACY

*But what are the rules?*

20

### INSIGHTS FROM A PRIVACY JOURNEY

*Lessons learned implementing the APPs.*



PRIVACY EDITION

# When is information really de-identified?



Participant anonymity is a fundamental of market and social research, one of the main elements that differentiate research from direct marketing. It is covered in Rule 10 of the new AMSRS COPB.

**The comment after Rule 10 states:**

*A researcher may disclose de-identified information freely, provided that there is no reasonable likelihood that the disclosed information could be used to identify one or more of the individuals who participated in the research, such as where the pattern of answers could reveal their identity*

So, what constitutes de-identification of information?

De-identification means a process of ensuring that identifiable research information is rendered permanently non-identifiable, i.e. without retaining a means

by which the information could reasonably be re-identified. It is intended to be a permanent and irreversible process.

Information held in some forms is virtually impossible to de-identify. Video recordings are always identifiable – pixilation of faces is not sufficient. Audio recordings are almost equally difficult to de-identify, as the content, tone of voice or figures of speech used may identify the individual.

Some techniques, such as the removal of identifiers on digital files, may be used to make identification more difficult, but if there remains a reasonable possibility of identification, (such as by matching two

**Video recordings are always identifiable – pixilation of faces is not sufficient**

sets of data) the information has not been de-identified.

Research involving small populations or a customer base is particularly problematic. We recommend against the provision or use of verbatim comments in projects involving these groups. Participants are often known personally to the client and he or she may recognise who has made a verbatim comment in a presentation or report.

So, sometimes it is just not possible to guarantee de-identification of an individual's information. In these cases, you must always handle the individual's information under the conditions laid out in Rule 10 or risk breaching the AMSRS Code of Professional Behaviour and the Privacy Act.

Note that the term 'reasonable likelihood' mentioned in the comment quoted above is also used in the Privacy Act. Whether any particular approach to de-identification meets the standard required in the context of the Privacy Act will be a matter to be decided on the facts.

**The Office of the Australian Information Commissioner's (OAIC) website has various resources to help you manage and minimise the risk of re-identification of personal information:**

**[www.oaic.gov.au/](http://www.oaic.gov.au/)**

JANE GREGORY, AMSRS PROFESSIONAL STANDARDS OFFICER

