

Privacy Impact Assessment

Executive Summary

This Privacy Impact Assessment (PIA) has been developed as part of a proposal for permitted research, by Crosby Textor Research Strategies and Results Pty Ltd (C|T).

As an entity that conducts research, C|T is seeking authorisation from the Australian Communications and Media Authority (ACMA) to use and disclose unlisted mobile number information, in accordance with the Telecommunications Regulations 2001. An application has also been submitted by C|T's field agency, EMRS.

The mobile number information will be used for research C|T will conduct on behalf of the Liberal Party of Australia to understand public opinion on a range of electoral and public policy issues.

The express purpose of the PIA is to ensure that C|T is taking all reasonable steps to ensure that our research project implements all best practices, procedures and systems to ensure full privacy compliance and identify better practices.

C|T will direct the project and fieldwork will be carried out principally by EMRS, a subsidiary of Crosby Textor Research Strategies Research Pty Ltd, through Computer Assisted Telephone Interviewing. As such, in performing the PIA, C|T has also tested privacy measures in place at EMRS.

Catherine Douglas, Managing Director of C|T's Australian research and campaigns business, was responsible for overseeing the PIA and in ensuring recommendations are implemented.

Findings & Recommendations

The PIA determined that operational procedures of C|T and its subsidiary EMRS were sufficiently robust to protect the privacy of individuals to which the mobile information belongs.

The process did identify a series of measures that will be put in place to further enhance privacy measures at C|T and ensure optimal security for the IPND mobile information:

- All relevant employees (those working electoral research for the Liberal Party of Australia) will be asked to sign a declaration acknowledging the conditions of the authorisation to use the IPND mobile information
- A separate IPND do not call register will be maintained by EMRS to ensure these mobile numbers are not mixed with other sample
- All relevant employees, at EMRS and C|T, will be briefed on the conditions for the authorisation prior to engagements commencing

- C|T will appoint an IPND liaison manager and institute regular reviews to ensure there has not been a breach and that controls are working and sufficiently robust
- [REDACTED]
- Telephone interviewer scripts will be updated to reflect the conditions of the authorisation and to ensure all disclosures are made
- C|T has uploaded its Australian privacy statement to its website:
<https://crosbytextorgroup.com/privacy-notice-au/>

Small amendments have also been made to C|T's onboarding materials, contracts and staff handbook to further formalise compliance measures.

Privacy Impact Assessment Methodology

C|T, in consultation with the Liberal Party of Australia, conducted this PIA following the guidelines set out by the Office of the Australian Information Commissioner.

The Privacy Impact Assessment was conducted over a period of approximately six weeks in November and December 2018 as a part of a routine compliance review of C|T's operations. Subsequent reviews of C|T's privacy measures have taken place in March and April, 2019

C|T carried out this appraisal with support from its UK based Chief Compliance Officer, Leah James, local compliance head of compliance, David Bell, and field agency, EMRS. It also received input from its consulting lawyer during the assessment.

Formal feedback was received by the ACMA and informal conversations have also taken place to help finalise the IPND application and privacy impact assessment.

In addition to its own internal processes, C|T regularly consults with external stakeholders. For example:

- All researchers at C|T are members of the Australian Market & Social Research Society of Australia (AMSRS). In addition to reviewing industry bulletins, team members attend relevant briefings and conferences to stay abreast of changes to the Code of Conduct and trends affecting the industry
- The C|T Group regularly consults its lawyers on matters related to privacy, both in Australian and other global markets
- As a UK headquartered consultancy, the C|T Group is also fully compliant with the General Data Protection Regulation, which requires extensive consultation with government and independent organisations

Project Description

The research project will be conducted through Computer Assisted Telephone Interviewing across federal and state electorates, for the upcoming federal election.

Through a series of different surveys, C|T will seek to understand the perceptions of Australian voters towards policies, candidates and parties. The likely social benefits to come from this research will be the formulation of public policies based on the views and preferences expressed by voters.

During the project, C|T will ensure that collection, use and disclosure of personal information is consistent with the Privacy Act 1988 and Australian Privacy Principles.

All of C|T's surveys are scripted. Unless a response is common sense, scripts are also provided to interviews to deal with specific scenarios arising on a call. If a respondent shares that they would not like to continue, the call is terminated and the information is destroyed.

The final form of this research will be delivered in PowerPoint presentation format to the Liberal Party of Australia, with accompanying anonymised data tables. The research and end product will be conducted in full compliance with the AMSRS Code of Professional Behaviour, and all local laws concerning data collection relevant to our business.

Privacy Considerations

During the course of a research interview, information from a respondent may be disclosed that identifies the individual. It may then be possible for an organisation to identify what a respondent says or thinks about a particular topic; in this case, how a respondent views a political representative, candidate, party or policy. Should a person be identified, it may be possible for them to be targeted with unwanted information by political parties or to have their views about a topic, organisation or person known when they do not wish for them to be.

The research project, like nearly all research undertaken by C|T, will be carried out on an anonymous basis. C|T takes a number of steps to ensure the identity of respondents is not revealed at any time during the process. To follow is an overview of the project information flows and security measures that are and will be in place to mitigate against any breach.

Project Information Flows

To follow is a description of how information will flow during the project:

- C|T IPND liaison, Michael Turner, will take receipt of the mobile information from the IPND manager
- [REDACTED]
- At the start of an engagement where C|T is conducting research into electoral matters for the Liberal Party of Australia, Michael will provide the mobile information to C|T's fieldhouse, EMRS
- The EMRS operations team will store the mobile information electronically, in a secure location where all files are also password protected
- When the engagement commences, only mobile phone numbers are loaded into the system – there is not any other identifying information

- The interviewer completes the interviewers for the engagement
- At the conclusion, the operations team de-identifies all information before sharing the research information with C|T
- The research information collected by EMRS is stored securely for up to a year (unless there is a requirement to keep the information for longer) at which time it is destroyed
- At no stage does C|T receive information from EMRS that has not been de-identified
- C|T receives information and stores it on a secure section of our network; all files are password protected
- Information stored by C|T is catalogued and reviewed annually to determine if it can be destroyed
- Within 10 days of the authorisation to use the IPND database ending, the mobile information will be destroyed both by EMRS and C|T

Project & Organisational Security Measures

- C|T will store the IPND mobile information in a secure location, [REDACTED]
- Once C|T shares the mobile information with EMRS, it is will be stored in a secure electronic location that only relevant members of the operations team can access; the files will be password protected to further restrict access
- All members of the C|T and EMRS teams coming into contact with the mobile information will be require to sign a declaration acknowledging they understand and will abide by the conditions of authorisation
- All research information collected using the mobile information is de-identified before it is shared with C|T
- Hardcopies are shredded immediately after use or placed in locked secure shredding bins. No material is left unattended either in the office or outside
- Entry to the office requires an electronic pass. All employees are briefed during ongoing and throughout their tenure on confidentially, which is also a condition of their contract
- EMRS conducts spot audits at the conclusion of each engagement to ensure there has been no breach of conditions
- Both C|T and EMRS maintain catalogues of personal information held, which is reviewed annually and destroyed if it is no longer needed
- C|T and EMRS conduct regular reviews of their IT system to ensure it can withstand a breach
- In the event any of the conditions relating to the authorisation are breached or may have been breached, the IPND liaison will be informed immediately
- If there is found to be a breach, use of the mobile information will cease immediately and the ACMA will be informed; the mobile information will not be used again until confirmation to proceed has been received from the ACMA
- If a breach occurs a review of all engagements will take place to ensure there has not been a further breach

As an additional measure, the Liberal Party of Australia has agreed with the C|T group that information will be provided directly by the IPND manager to the C|T Group, rather than to the Party.

Conclusion

In summary, C|T has rigorous processes in place to effectively manage privacy of individuals' data.

Through this impact assessment, C|T has taken action to further document and formalise business practices related to destruction of data, onboarding procedures and routine changing of passwords. This includes:

- Amending scripts for CATI interviews and focus groups
- Updating and distributing an employee handbook
- Updating employee contracts
- Updating the privacy policy
- Providing instructions on changing of passwords
- Declaration for relevant employees acknowledging the conditions of the IPND authorisation
- A separate IPND do not call register will be maintained by EMRS
- Appointment of an IPND liaison manager
- Separate electronic storages spaces will be created both at C|T and also EMRS for the IPND mobile information
- C|T has uploaded its Australian privacy statement to its website:
<https://crosbytextorgroup.com/privacy-notice-au/>

Appendix 1

About the C|T Group

Founded by campaign strategists Sir Lynton Crosby and Mark Textor, the C|T Group offers a world renowned brand of successful, research-driven campaigns.

The C|T Group combines decades of experience in research, political campaigns, strategic communications, media, and corporate intelligence to deliver winning strategies at the highest levels of business and government.

Having worked on successful election and corporate campaigns across four continents, we understand the need for timely, actionable intelligence, so our clients can focus the right message and resources on their most persuadable 'swing voters' to get the results they want.

Our team of over 80 international, multilingual staff operate from offices in London, Sydney, Canberra, Milan and Washington D.C.

Research

The C|T Group believes in providing answers, not just information. A successful campaign knows which audience will decide the outcome, where they are, what they think and how to communicate with them. This is why cutting-edge opinion research is at the heart of our business.

Traditional research approaches will tell you what people think, the C|T Group's method is to find out why they think it. These insights allow us to create values-based campaign strategies that are rooted in fact and are emotionally resonant with our clients' target audiences.

Our research-driven approach has been successfully deployed in campaigns across the globe, whether in national elections, corporate positioning, complex financial transactions or brand architecture development.

The research services we offer include:

- Public opinion polling
- Focus groups and in-depth interviewing
- Corporate image and brand research
- Financial transactions research
- Shareholder research
- Employee and workplace culture research
- Telephone and online canvassing

EMRS

The C|T Group also owns fieldhouse, EMRS. EMRS collects all data in-house, through its own call centre with its dedicated team of trained interviewers, its fully hosted online research offering, and its focus group facilities in Hobart.

Resources and capabilities:

- 5 seat in-house call centre
- Auto dialler calling landline and mobile phones

- 90+ fully trained call centre interviewers
- Senior call centre supervisors ensuring rigorous training and monitoring of interviewers
- Fully functional online research offering
- Email distribution of online surveys and reminders
- 100% control with 'live' data quality checks and updates to clients
- Our own EMRS Tasmanian panel of pre-screened adults who have agreed to participate in online surveys