

Terms

attentionTRACE™ or App—refers to the software application developed by Amplified Intelligence

Cookie—a text file that a web browser stores on a user's device to recognise the user and store their information and preferences

Policy—means this privacy policy

Context

Amplified Intelligence (Amplified) is a research company and, as such, relies on the participation of people who are willing to share their data with us. While our work is measured in numbers, we never forget that people are behind those numbers. We understand the importance of the data we hold; it's importance to you and to us. For this reason, we treat it with respect and gratitude.

Purpose

This Privacy Policy explains how Amplified collects, uses and protects your personal data. It is also our declaration that we will respect your rights under the Australian Privacy Principles contained in the Privacy Act 1988 (Cth), as well as under the EU General Data Protection Regulations and as a global digital citizen.

We are required to comply with the General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) to the extent that we receive information regarding persons in the European Union about their behaviour as it occurs in the European Union. Amplified is a data controller and a data processor for the purposes of the GDPR.

This Policy applies to Amplified Intelligence website users as well as all respondents who agree to participate in Amplified Intelligence research that involves downloading and installing to their mobile device or computer a software application (attentionTRACE™) developed by us.

Privacy Contact

If you have any questions about our policy or your data, feel free to contact our Data Privacy Officer.

Data Privacy Officer: Dylan Lundy, Senior Software Engineer
dylan@amplifiedintelligence.com.au
Amplified Intelligence Pty Ltd
Lower Ground, 28 Franklin Street
Adelaide SA 5000

Amplified Intelligence Research Services

Why we use your data

Amplified uses your data to conduct media and marketing research to determine the effectiveness of media and advertising across different platforms.

About attentionTRACE™

The attentionTRACE™ App is free of cost and, as such, collects no personal financial information.

*Please note, if ever a charge is made against your bank account for the App, it is fraudulent and must be reported to your financial institution immediately.

If the participant forgets to remove the App it remains dormant. It does not engage for any further activity after the research process is complete. It becomes redundant. attentionTRACE™ does ask participants to log in to various platforms (e.g., Facebook and Instagram), but DOES NOT scrape any personal log in data.

Sharing your information

Amplified is grateful that there are people willing to participate in our research. We take custodianship of this data very seriously.

We do not and will not sell your data to any other party. Your data may be shared with a third party such as the case for storage. In this case, we ask assurances from that third party that they will not on-sell your data and that they meet the EU GDPR requirements.

Collecting personal information

Amplified does not collect personal information other than as is specified in this Policy. We collect all data for our research through accredited panel providers. Personal identifying information remains with the panel provider.

Amplified assumes that you have registered with the panel provider in full knowledge of their data and privacy policy. By downloading attentionTRACE™ you consent to us processing your facial recognition data and you acknowledge that we do this legally under the conditions of our contract with the panel provider.

Participants are reminded twice during the research process that they are being filmed.

Whilst images and video of your face may be recorded, this is stored in a de-identified manner, with the only identifying feature being a unique ID number assigned to the video or image.

After panel collection Amplified receives video footage of the people who have agreed, with the panel provider through a double opt-in process, to participate.

Access to your information

Requests for access to your data held by Amplified must be made initially through your panel provider. They will be able to provide the unique identifier that will enable us to locate your video footage.

Opting out—removing the App from your device

The App is designed to be made redundant when the data collection phase for the research project is complete. As such, it is sequenced and relies on the final step being completed. If a participant wants to opt-out of the project part-way through, they can use the steps specific to their device for removing the App.

If you are not able to quickly and easily opt-out from data collection, we can and will help you if you ask. If you have any questions regarding removal or opting-out, contact our Privacy Officer at dylan@amplifiedintelligence.com.au

Cookies

The App does not use cookies. Please note that our third party panel providers may use different types of cookies for your registration process with them. For information about this, you will need to read their Cookies Notice or the Cookies section of their privacy policy.

The information we hold

Amplified does hold video footage of the faces of participants. This data has no personal identifiers associated with it. Rather, it is tagged with the participant's unique panel provider number.

How we use your data

Amplified receives facial video footage from its panel provider, which we run through our machine learning model to create research outputs. That is, we look at numbers not faces.

Amplified staff review video footage occasionally when required to improve or solve problems within the research framework, or when we train the machine learning models.

We use your data in the following circumstances:

- To undertake research contracts as briefed by clients of Amplified
- Where we need to comply with a legal or regulatory obligation
- To assess the performance of our own research framework and products for the purpose of improvement
- To develop new service offerings.

Third party agreements

Amplified maintains arrangements with third parties to:

- manage the selection and registration of participants
- manage the discrete choice methods survey part of the research
- store and secure data.

At times it is obvious to research participants that a third party is involved, for example, with the panel provider. At other times, it is not obvious, such as delivery of surveys.

In the event that we engage a third party to process the personal data of persons in the European Union on our behalf, it will only do so if that third party has provided assurances that it will implement procedures in compliance with the GDPR, and the protection of the personal information of persons in the European Union.

Amplified maintains arrangements with a third party for data storage and security of data. This data storage facility is Amazon Web Services based in Sydney, Australia.

Data security and retention

Amplified does not have access to personal information other than that listed in this Policy. All personal identifiers are collected by our third party panel providers. After panel collection Amplified receives video footage of the people who have agreed, with the panel provider, to participate through a double opt-in process.

For the data we do have, Amplified has appropriate security measures (via a third party) to prevent this data from being accidentally lost, used or accessed in an unauthorised way. We will take all reasonable steps to secure your data, however we cannot guarantee that it will be completely safe from attack by malicious parties.

We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

Using our website

Collecting personal information

Amplified does not collect personal information without individual consent. You will be asked to accept our Cookies Terms of Use before proceeding to browse our website.

The information we hold

We will collect information relating to you as a website user and not as an individual. We will use this data solely for statistical purposes to improve the performance of our website. This information may include your server's address, top level domain name, date and the time of your visit, pages downloaded and the browser used. No attempt is made to identify individual users on their browsing activity.

Cookies

When you visit www.amplifiedintelligence.com.au, we may use a 'cookie' to make a record of your visit and log information for statistical and administrative purposes.

You may remove cookies and/or control their operation by adjusting your browser settings.

Third party agreements

This Privacy Policy does not cover the information practices of third parties, nor their collection and use of personal information even if they are linked to our website. Please refer to the privacy policies and statements of linked service providers and obtain information regarding their collection, use and disclosure policies.

We have no influence on the third party website content and are not held accountable for their correctness. The owner of that website carries the responsibility of its content. We dissociate ourselves distinctly from all the content of all linked pages on this site.

We may disclose information to service providers retained to perform website analytical services on our behalf. These service providers are asked to treat this information as confidential and are prohibited from using the information for purposes outside instructions from Amplified.

Data security

Data regarding the use of the www.amplifiedintelligence.com.au is collected and stored by Google Analytics.

Please keep in mind that sending your information over the

Internet is not completely secure. In particular, email sent to or from the Amplified website may not be secure. Please choose carefully the type of information you send to us via email.

Your rights

In addition to the protections afforded under the Australian Privacy Act and the APPs, if you are a European Resident, you have a number of additional rights under the GDPR, including:

- the right to receive personal data you have provided to us in a structured, commonly used and machine readable format, including the right to request that we transmit this data directly to another data controller
- the right to restrict the processing of your personal data in certain circumstances
- the right to require us to erase your data in certain circumstances.

Your additional rights as an Amplified Intelligence research participant include:

- the right to opt-out at any time, although there may be some loss of incentive depending on your agreement with the panel provider (please check with them).

If you would like to modify or remove personally identifiable information, please note that your specific request should be made to the panel provider in the first instance as they will have your unique identifier number. Once we have your unique identifier, we can locate and delete or move your information.

How to make a complaint

If you have a question about this Privacy Policy or a complaint about how we have managed your personal information, we would like hear from you. Contact our Data Privacy Officer, because if there is any way we can explain the reasons or fix the problem, we will. Plus, it gives us the opportunity to re-evaluate our processes.

If after we've worked together, you still feel as if your complaint hasn't been resolved you can contact the Office of the Australian Information Commissioner. Here are a few ways to do that:

Telephone: 1300 363 992 (local call cost, but calls from mobile and pay phones may incur higher charges)

Telephone (from overseas): +61 2 9284 9749

TTY Hearing Impaired Telephone: 1300 363 992

Translating and Interpreting Service: 131 450

Post: GPO Box 2999 Canberra ACT 2601

Online Enquiry Form