

Introduction

Amplified Intelligence (Amplified) is a leading research technology company in providing transparent and accountable metrics and solutions to the advertising and media industry. As such, we rely on the participation of generous people who are willing to share their data with us. For this reason, we set a high standard for consent and we take your fundamental right to privacy and the respect for, and compliance with, all global data protection laws, very seriously.

It is our declaration that we will respect your rights under the:

- Australian Privacy Principles contained in the Privacy Act 1988 (Cth),
- The EU General Data Protection Regulations General Data Protection Regulation (Regulation (EU) 2016/679)
- The Californian Consumer Protection Act CCPA

In summary, all of these laws revolve around protecting you and your:

- Right to know about the personal information we collect about you and how it is used and shared;
- Right to delete personal information collected from you
- Right to informed and explicit consent
- Right to opt-out, and/or limit, the sharing and/or use of your personal information; and
- Right to non-discrimination
- Right to correct inaccurate personal information

Amplified Intelligence acts as a data controller and a data processor. This Global Privacy Policy applies to both Amplified Intelligence panellists and website users.

If you have any questions, concerns or comments about this Global Privacy Notice, or you believe your personal information has been used in a way that is not consistent with the Global Privacy Notice or your choices, you can contact our Privacy Team, via email or postal service, at:

Email: DPO@amplifiedintelligence.com.au

Postal: Amplified Intelligence Technologies Pty Ltd, Level 1, 109 Grote Street Adelaide, South Australia, 5000

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, at:

Email: enquiries@oaic.gov.au, Postal: GPO Box 2999 Canberra ACT 2601

1. PARTICIPANTS OF OUR PANEL BASED RESEARCH

Why we use your data

Amplified uses your data to conduct media and marketing research. This research helps the industry determine the effectiveness of media and advertising across different media platforms. Some of this research involves panellists downloading and installing a software application (attentionTRACE) developed by us, in some cases research involves receiving hardware through the postal service.

About attentionTRACE

The attentionTRACE app, Amplified software and/or associated hardware is free of cost. In fact, we pay you for your time! We are grateful for your involvement and all panellists are generously remunerated via our panel partners (we never collect bank account details or personal financial information).

You can only be recruited, and download our app, through our certified panel partner and we collect lawful basis to process such Personal Information is your consent.

Collecting your personal information

We are interested in how you interact with and use media and all data collected from our apps is used only for this purpose. To do this we undertake gaze tracking and we collect some media and device usage information about how you interact with media.

This is all done with your consent given on multiple occasions.

What this means is that, when you consent to download attentionTRACE, or have an attentionTRACE mediahub in your home, you will be asked to consent to us collecting and processing video footage through the device camera only for the purpose of eye tracking and only when you are consuming media. Think of it like a Zoom call when it asks your permission to turn the camera on in advance of it doing so, except our consent process requires your opt in three times (so there are no accidental approvals). Other non personal data collected includes volume, scroll speed and media configuration (i.e. how the Facebook feed works) from the mobile app and the TV app collects a condensed audio fingerprint of what sound is on the TV.

But that's it. It does NOT passively track you in the background.

It does NOT scrape social media posts, social handles, conversations, private messages, phone calls, your personal phone number, texts, other apps or online browsing. Personal identifying data such as name and contact details remain with the panel provider (unless you are receiving a package in the postal service, then you choose if you want to give us this information). Demographic questions are not mandatory to provide. We do not ask you about your ethnicity, religious beliefs, sexual orientation, political opinions, health data or criminal convictions and offences.

We do not identify you, or make inferences about you as a unique individual in any way.

Amplified assumes that you have registered with the panel provider in full knowledge of their data and privacy policy and you will be asked to acknowledge that we do this legally under the conditions of our contract with the panel provider.

Sharing and storing your personal data

We take custodianship of this data very seriously and we use your data in the following circumstances:

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

In the case of data usage number 1 and 2, any personal data is analysed at an anonymised and aggregated level (i.e. not person-level).

This means that any biometric data effectively becomes 'zeros and ones' to our analysts and clients.

We do not, and will not, sell your personal data to any other party. We do not use your personal data for targeting purposes. We only use it for research purposes to gain insights on effectiveness of media and advertising across different platforms. Amplified maintains formal agreements with third parties to:

- Store and secure your data.
- Manage the selection and registration of participants
- Manage any survey components as part of the research

We ask assurances from third parties that it will implement procedures in compliance with the GDPR, and the protection of the personal information of persons in the European Union.

Please be aware that the Personal Information we collect may be transferred to and maintained on servers or databases located outside your state, province, country, or other jurisdiction. To ensure our Websites and Reporting Tools are efficient and responsive, Amplified Intelligence generally stores all Personal Information collected through our Websites, Sales Activities and Reporting Tools in Sydney Australia (AWS). Please see [this link](#) for their elevated security procedures and infrastructure.

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In the unlikely event of a personal data breach we will notify your panel provider and any applicable regulator of a breach where we are legally required to do so. While Amplified does hold video footage of the faces of participants, this video footage is stored and processed in a secure and de-identified manner with the only identifying feature being a unique ID number assigned to the video or image. This unique ID number is an arbitrary internal number we give viewing sessions, we do this so we can identify your data in an anonymous way. This means even with facial footage, we can't uniquely identify you as a person anyway.

We hold all personally identifiable data for 10 years.

While on occasion Amplified data controllers and processors review de-identified video footage, it is kept to a minimum and only when it is required to improve or solve problems within the research framework, and these employees are subject to a duty of confidentiality. General Amplified employees do not have access to this data.

Right to withdraw and objecting to processing

After any mobile media viewing session, the app becomes dormant. Even If you forget to remove the App, it does not engage for any further activity.

If you are part of a TV study the attentionTRACE media hub will only be on when the TV is on and we will be sending you regular requests for your ongoing consent.

If you want to opt-out of the project part-way through a viewing session, stop what you are doing and use the steps specific to your device to remove the App, or simply turn off the media hub.

If you wish to withdraw consent, modify or remove personally identifiable information about you please email hello@amplifiedintelligence.com.au and we will take action as you wish immediately.

If you have any questions regarding removal or opting-out, contact our Data Privacy Officer dpo@amplifiedintelligence.com.au

Cookies

The attentionTRACE App does not use cookies, and it does not passively collect non consenting data in the background.

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.

2. CUSTOMERS OF OUR TECHNOLOGY SOLUTIONS (attentionPROVE®)

Purpose

Our measurement technology serves both advertisers and media sellers by providing independent, third-party impression-level measurement.

While standard technologies that use only impression-level measurement have helped to improve online advertising standards for advertisers from a 'viewable' perspective, the gap between impressions that are viewable versus seen by a human is vast. The encrypted data we collect from consenting panel members worldwide continuously train the data we collect at an impression-level via JS Pixels. This produces highly accurate models that can predict human behaviour and the subsequent effectiveness of media and advertising across different platforms.

Our lawful basis for this type of processing of JS Pixel related information is based on our legitimate interest to pursue these goals.

About attentionPROVE

As a component of advertising tracking and reporting, our JS pixel gathers page views and impression data to offer media analytics services. This includes monitoring such things as browser information, device type placement dimensions, time on screen plus information about website characteristics, domain name, visiting day and time, and visited script URL(s). Our tracking spans multiple web domains owned or operated by different sites.

Collecting personal information

The attentionPROVE JS pixel does not store, record, read or collect cookie information.

Our JS Pixel does not collect contact details, scrape social media posts, social handles, conversations, private messages, phone calls, personal phone numbers, texts, other apps or online browsing.

It does not collect ethnicity, religious beliefs, sexual orientation, political opinions, health data or criminal convictions and offences.

The only Personal Data collected when this technology is deployed are the following:

- IP address

This personal information is not used to identify viewers, or make inferences about viewers as unique individuals whose impressions have had an Amplified pixel appended to them.

Sharing and storing your personal data

We do not, and will not, sell your personal data to any other party. We do not use your personal data for targeting purposes. We only use it for research purposes to examine impression data of ads served in addition to reporting viewability metrics of ad units across digital media sites. Amplified maintains formal agreements with third parties to:

- Store and secure your data.
- Manage the selection and registration of participants
- Manage any survey components as part of the research

We ask assurances from third parties that it will implement procedures in compliance with the GDPR, and the protection of the personal information of persons in the European Union.

Please be aware that the Personal Information we collect may be transferred to and maintained on servers or databases located outside your state, province, country, or other jurisdiction. To ensure our Websites and Reporting Tools are efficient and responsive, Amplified Intelligence generally stores all Personal Information collected through our Websites, Sales Activities and Reporting Tools in Sydney Australia (AWS). Please see [this link](#) for their elevated security procedures and infrastructure.

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In the unlikely event of a personal data breach and will notify your panel provider and any applicable regulator of a breach where we are legally required to do so. While Amplified does hold video footage of the faces of participants, this video footage is stored and processed in a secure and de-identified manner with the only identifying feature being a unique ID number assigned to the video or image. This unique ID number is an arbitrary internal number we give viewing sessions, we do this so we can identify your data in an anonymous way. This means even with facial footage, we can't uniquely identify you as a person anyway.

We hold all personally identifiable data for 5 years.

3. VISITORS TO 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 lawful basis to process such Personal Information is your consent.

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.