

# Augmented reality – a leap into a new world

---

**Olivia Whitcroft,  
Principal of OBEP,  
discusses the privacy  
implications of the  
increasing use of  
augmented reality  
technology**

---

**A**ugmented reality is a world that sits somewhere in between virtual reality and 'real' reality. It is frequently compared to the Terminator's abilities from the films of the same name, in which Arnie (presumably having purchased Google Glass) can see computer-generated information about the person he is looking at superimposed in front of his eyes on top of the real world.

My analogy is to an alternative sci-fi programme from the 1990s — Quantum Leap. In the episode 'Pool Hall Blues', Sam (our hero) has taken over the body of a great pool player and must win a pool match. The only trouble is, Sam (although multi-talented), is not very good at pool. But help is at hand! Sam's friend from the future, Al (who appears in the form of a hologram) is connected via a handlink to the supercomputer Ziggy, who can calculate the precise angles of the shots which Sam needs to make in order to pot the balls. The handlink, shaped much like a multi-coloured smartphone, projects the lines of shooting onto the pool table (seen only by Sam) and Sam follows them to win the match.

Augmented reality technology is already widely used in smartphone and tablet applications. These applications use our device (the handlink), to gather information about our surroundings (the pool table). This information is then passed via the internet from our device to another computer (Ziggy) containing a vast amount of additional data. The data are tailored to our needs and then shot back across the internet (admittedly through space rather than time), and projected onto our device's screen in front of the real world seen by our camera.

The technology enables an application to recognise the outside world using geo-location data or visual markers such as a QR (Quick Response) Code or other symbol. These are detected by the camera, GPS or other inputs on our device and then interpreted by the application. The resulting information which is then overlaid onto the real world may be images or words, or other sensory input such as sounds, depending on the technology. Users may then be able to interact with the augmented output.

This is used in many consumer applications, including games (for example for players to zap ghosts or zombies in

the garden) and providing useful facts and figures (such as enhancing maps, measuring objects or recognising star constellations). Augmented reality is also widely used in marketing and tourism materials (such as the new Ikea catalogue), enabling consumers to visualise and test products, providing tours around a shop or location, or overlaying printed information with virtual information such as translations, reviews and special offers.

A Google search also reveals that augmented reality projectors have been developed to draw out lines of shooting in a game of pool!

## Privacy and data protection in an augmented world

The privacy and data protection impacts of augmented reality are an extension of those we already face in the data rich world we have been living in for a while. As we go about our daily lives, our smartphone is never more than an arms length away, enabling us to share where we are, what we are doing, who we are with and what we look like whilst we are doing it. This information is fed into a huge databank of information on the internet, and may be linked to other data, analysed, and then used by organisations to provide information, create profiles, improve service offerings and send targeted advertisements.

Augmented reality is speeding up collection and delivery of information even more, and improving the quality of such information. The technology uses our mobile device to collect information without us needing to type it in, and can then project information right in front of our eyes rather than waiting for us to log in to our email to find it. This changes the nature and potentially the purpose of data processing activities, and exacerbates the associated privacy and data protection concerns.

## Who needs to be concerned?

All parties involved in the use of augmented reality technology and associated data need to be concerned about the privacy issues. This will include: the creator of the underlying technology; the organisation using

*(Continued on page 8)*

[\(Continued from page 7\)](#)

the technology to provide information or resources to end users; and any other party obtaining or using data as a result, such as an end user of an application or an advertiser. A complex data controller/data processor analysis may determine precisely where the legal responsibilities lie. However, it may be more practical for each party to focus on the desired outcome — to respect privacy and protect personal data.

## Privacy by design

Technology is rapidly becoming more sophisticated in its amalgamation and analysis of data leading to previously un-encountered privacy concerns. Looking into the future, the glasses we wear may 'recognise' passers-by and provide us instantly with associated biographical information, news articles and social media profiles. It will not just be celebrities whose privacy is threatened in public. Privacy and data protection issues should therefore be taken into account at an early stage of development of the technology and associated equipment and software. The use of privacy impact and risk assessments are key to identifying practical problems and how to address them within the design and implementation of the technology. Privacy by design and default, and the use of [data protection] impact assessments by data controllers and processors are also areas of focus within the proposed new EU Data Protection Regulation. Proposed duties for producers of technology were recently removed, but they will still have a part to play in practice.

## Transparency

There is a growing problem of how effectively to inform individuals how data about them are being collected and used. Describing complex data processing activities within a complex privacy policy does not solve this problem. Assuming an individual has taken the time to peruse such a policy (which in itself may rule out a lot of people), those who digest and understand it may be limited to data protection practitioners who are

looking for ideas for their own policy.

There therefore needs to be focus on clarity and simplicity in the presentation and content of privacy notices. This should take into account how obvious the data collection is and how privacy-intrusive the resulting activities are. Aside from compliance issues, individuals are likely to be more tolerant of actions they were expecting than those which, from their perspective, were taken without their knowledge.

Augmented reality technology is capable of being less obvious in its collection of data and more intrusive in its use of data than more familiar activities. For example, an organisation producing a conventional paper marketing brochure may only have the name and postal address of those to whom the brochure has been sent, and details of products they subsequently ordered. Add augmented reality, and the organisation can now analyse the type of device a person has, where they have been, which products they considered, how long they spent browsing, how they interacted with the content, and any comments or feedback they provided.

These details may also be linked to other data such as social media profiles, and include information about other individuals associated with the user. The combined data set may be used by the organisation and shared with third parties or other users. The result can therefore be a complex mix of processing activities, the means and purposes of which are partly conventional and partly new technology.

Improved clarity could potentially be achieved through use of standard expressions or icons which are easily recognised by consumers. A concept along these lines is used by Google Play Store, which provides a summary of standard 'App Permissions' before an application is downloaded. However, there is a long way to go in achieving a clear common approach to privacy notifications. Widespread co-operation (between organisations, industry bodies and/or regulatory authorities) would be needed to set up standards and ensure consistency in the approach used.

## Obtaining consents

There is a similar challenge in obtaining effective consents for data processing where required, for example in relation to marketing, behavioural analysis, data sharing activities or perhaps the use of augmented reality features at all. A consent is highly unlikely to be effective if, in practice, the description of the activities to which the consent relates was not seen or understood. As noted above, aside from legal compliance, consumers are likely to be less tolerant with more intrusive activities. Consent wording which is craftily drafted and presented so as to 'trick' users into agreement is unlikely to result in happy customers.

'Intrusive' may come in different forms. It may be a targeted advertisement which flashes up in front of a consumer's eyes. Taking this a few steps further, it may be the ability to recognise an individual as they walk along the street and provide others (whether for personal interest or commercial gain) with augmented versions of that individual. This may include information about that individual's activities and behaviours.

As use of augmented reality technology and the associated data processing grows, it may assist if individuals have the ability to give blanket opt-ins or opt-outs to specified privacy-intrusive activities by any organisation. There are significant challenges ahead in setting up, monitoring and enforcing such a scheme.

## An augmented future

As augmented reality become more commonplace and the associated use of data more standard, there is hope that privacy and data protection practices will also adapt and evolve, and consumers' expectations with them. No doubt there is a lot more discussion to come in this area, both from a privacy perspective and wider legal and social concerns, such as cheating at pool.

---

**Olivia Whitcroft**  
OBEP

olivia.whitcroft@obep.co.uk

---