

Augmented privacy: with progress comes responsibility



EXPERT ARTICLE

_DANIEL NEUBIG

AR Technical Lead

Ergon Informatik AG

_URS ZURBUCHEN

Senior Security Consultant Airlock

Ergon Informatik AG

Published in SMART insights 2021 magazine

ergon

smart
people –
smart
software®

The pandemic has forever changed the way we communicate and collaborate. It has also encouraged us to explore augmented reality, giving it a considerable boost. Now market-ready, AR has a whole array of uses but the technologies it needs conflict with important issues – primarily data protection. Any enterprise using AR has a responsibility to tackle these risks early on.

Co-working and social contact have increasingly moved into virtual spaces over the past year. As we have adopted distributed working, we have turned in a big way to digital communications, video conferencing and also projects that use augmented reality (AR).

The solutions offered by market leaders such as Microsoft, Apple, Google, Facebook and Amazon push the benefits for commercial users and point to massive market potential. Meanwhile, new AR applications are popping up everywhere to improve or simplify existing products. They are being incorporated into all sorts of exciting projects and acceptance is high. Analysts expect the AR services market to grow by 100 per cent annually.

Augmented reality has a lot in its favour for both corporate and individual users but the new technologies unfortunately carry risks and potential liabilities, too. They use sensitive personal data that might be subject to all manner of legislation and raise questions of data privacy and security. Companies are responsible for recognising this from the start in their digital strategies.

The role of data

AR makes it much easier for users to access digital content from products and services across many sectors. Imagine tourists exploring with a virtual guide that gives them details of nearby attractions, the way AR enables construction elements to be positioned more quickly in industry, or how computed tomography models can be projected onto a patient during surgery.

Augmented reality gathers information from a variety of sensors – not just location and video but also biometric data and other personal information. The scope and availability of this information determines the accuracy of the virtual world and thus its practical benefit.

However, people are becoming increasingly conscious of who is using their data and what for. There is also a growing realisation that situations or conversations, which we assume to be personal, are not nearly as private as we think. Unsurprisingly, society is becoming sceptical. This distrust can put an abrupt end to the enthusiasm elicited by a new product and make it difficult to adapt to emerging opportunities. There is uncertainty about what happens to data once it has been collected and how effectively it is protected.

Inappropriate use in an uncontrolled and unauthorised context is a particular worry. In many cases, AR collects information on unrelated third parties, such as faces in the background on a photo, and users do not suddenly want to be facing liability actions or damages claims.

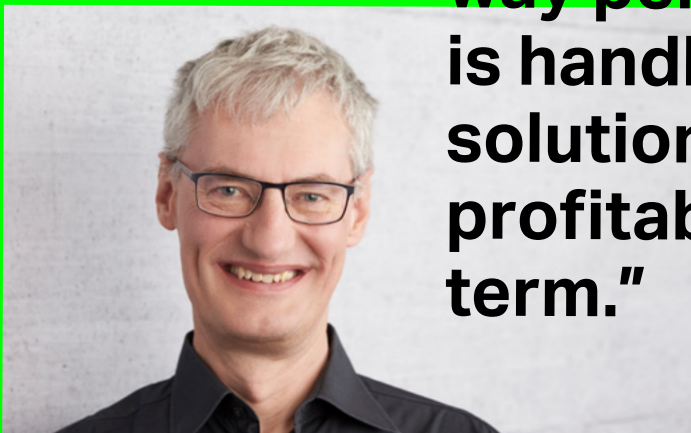
The privacy aspect of data protection is nothing new. Whether we're conscious of it or not, it is part of everyday life, with sensitive data processed and stored by social media, wearables, smartphones, Internet of Things devices and smart homes. Machine learning algorithms recognise patterns in this mix of sensor data, images and videos, and make assumptions and decisions. Many of us have got used to this and are willing to accept the potential risks in return for greater comfort and convenience. The software is making life easier, after all. A company's reputation is a major factor here. The more ethical and credible its pledge, the greater the consumer's trust and willingness to share. Many of the functions of AR cannot be used without such personal data. The unique thing about these solutions is that they combine all the data into a single platform. Aggregation improves the accuracy and quality of the data that has been collected, for

"Transparency and conscious decision-making allow users to opt for a more private risk profile in return for compromises on functions or accuracy."



_DANIEL NEUBIG, AR TECHNICAL LEAD;
DANIEL.NEUBIG@ERGON.CH

"Monitoring the market and continual adjustments to the way personal data is handled will ensure solutions remain profitable in the long term."



_URS ZURBUCHEN, SENIOR SECURITY CONSULTANT AIRLOCK;
URS.ZURBUCHEN@ERGON.CH

The benefits of augmented reality

BUSINESS CASE	BENEFITS AND EXAMPLES
AR NAVIGATION	- EASY TO FIND LOCATION AND ATTRACTIONS - DIRECTIONS, E.G. TO A RESTAURANT OR WITHIN A LARGE BUILDING
ADDITIONAL INFORMATION ON THE REAL WORLD	- RECOGNISES USER INTENTION AND ADJUSTS INFORMATION TO THE SITUATION - FASTER INTERACTION WITH OBJECTS AND FUNCTIONS - SIMPLER AND MORE CONTEXT-SENSITIVE TO USE, E.G. TO PLAN INTERIOR FITTINGS - INFORMATION AVAILABLE ON SITE (STOCK LEVELS IN RETAIL, MAINTENANCE AND OPERATION OF IOT DEVICES)
ENTERTAINMENT	- VIRTUAL CONTENT WHEREVER YOU ARE, E.G. POKÉMON GO - SHARED CONTENT
REMOTE COLLABORATION	- REMOTE COLLABORATION WITH A VIRTUAL PRESENCE - SHARE YOUR OWN VIEW AND WORK WITH THE TEAM BUT FROM A SAFE DISTANCE - FAST, INEXPENSIVE EXPERT SUPPORT, E.G. TELEMEDICINE OR MACHINERY MAINTENANCE AND OPERATION
TRAINING	- IMMERSIVE INTERACTION IN A VIRTUAL SPACE - SIMULATION OF EXTREME SITUATIONS - PERSONAL EXPERIENCE IMPROVES THE TRAINING OUTCOME - PSYCHOLOGICAL TRAINING TO COMBAT ANXIETY, FOR EXAMPLE

The risk of augmented reality applications

ORIGIN	RISKS FROM UNWANTED DATA USE
PERSONAL/CUSTOMER-IDENTIFYING DATA (PID/CTD)	- EXACT MOVEMENTS RECORDED - PERSONAL IDENTIFYING/BIOMETRIC DATA - E.G. SENSITIVE PATIENT DATA - HACKING - PROFILE AND AVATAR HIJACKED - SOCIAL ENGINEERING - PROFILING AND TARGETING - ATTENTION TARGETING - MANIPULATION
SPATIAL CONTEXT	- PUBLIC SPACE AND WORKING ENVIRONMENT - PRIVATE / SEMI-PRIVATE SPACE WITH PERSONAL DETAILS - SURVEYING AND RECORDING OF LOCATIONS AND SPACES
SITUATION CONTEXT	- PRIVATE OR PROTECTED CONTENT SHARED UNKNOWINGLY - SENSITIVE RECORDING IN THE BUSINESS ENVIRONMENT; LOCATIONS, PRODUCTS AND CONVERSATIONS
UNRELATED THIRD PARTIES	PERSONAL RIGHTS OF PASSERS-BY
VIRTUAL CONTENT	- BREACH OF COPYRIGHT - ONLINE HARASSMENT - ABUSIVE CONTENT
CROWDSOURCING	- CONTENT MODERATION - FILTERS - COPYRIGHT AND OWNERSHIP

facial recognition or location tracking, for example. Unlike other applications, AR sensors record constantly and in real time, not just selectively in predefined situations. And because it captures not only the user's actions and reactions, but also the situations that trigger them, along with the context, AR even gives clues to unconscious and passive behaviours.

Not just an ethics issue

Where a company uses AR to optimise its own processes or as part of its offering, there is even more of a duty to handle data responsibly. It is important to communicate transparently about how the collected data is secured, and how it is used. This allays fear and builds trust.

There is little reliable guidance here, either for the present or, more importantly, the long-term future. Depending on region, regulations and security standards are at different stages of maturity. Their structure and scope also vary. The continuous increase in awareness of data privacy indicates that the public remains undecided. Things that are accepted today may cause outrage tomorrow.

Amid the confusion are efforts by organisations such as XR Safety Initiative (XRSI) or OpenARCloud to create a self-regulatory framework to provide information and determine best practices. It is crucial to the long-term profitability of AR solutions that questions of personal data privacy are addressed proactively. It is a balancing act between allowing innovation while avoiding potential reputational damage, and securing the investment received and the profit it generates.

Companies embarking on AR projects are advised to take the privacy-by-design approach: protections for sensitive data are not merely an add-on in the application design and development phase, they are guaranteed from the start. Data collection is reduced to what is permitted, necessary and useful, and data is not stored if it is only used in the short-term. Access controls and encryption are key here to keep things on a need-to-know basis.

Informed consent

Absolute transparency about what data is recorded and how it is used is critical. This is best done by involving users and giving them choice – a more private risk profile in return for compromises on functions or accuracy, for example. Depending on the scenario, this informed consent can even be restricted to a specific situation, along the lines of “may the facial recognition cloud service analyse this video image for the next five minutes? Yes/no – more info”.

This is no place for text-heavy declarations of consent and T&Cs. Users are unlikely to read them anyway. Animated or even interactive instructions and tutorials in the application context itself are better options. At the same

time, the company publishes the relevant guidelines and codes of conduct, and undertakes to abide by the same rules. You may have seen this in practice on communication platforms and social media, where it is common. The future will bring still further applications that will determine how we work and interact with each other.

Focusing on strengths

Augmented reality has the ability to take the user experience to the next level and thus the potential to be a huge hit on the market. It nonetheless carries a variety of risks, especially where personal data is concerned and from a long-term perspective. That is why it is imperative that users are informed clearly and comprehensibly about how their personal data is used, and that they have freedom of choice. Data-consciousness will continue to grow. With that in mind, we may find that consumers begin to question products only well after their launch. To anticipate such changes, and be able to respond to them appropriately, companies are handing market monitoring over to experts at the forefront of technological development who are quickly able to interpret its effects on security and privacy. />

Interested in more?

Digitisation projects
Change makers
Tech trends

Order now
ergon.ch/smart-2021

