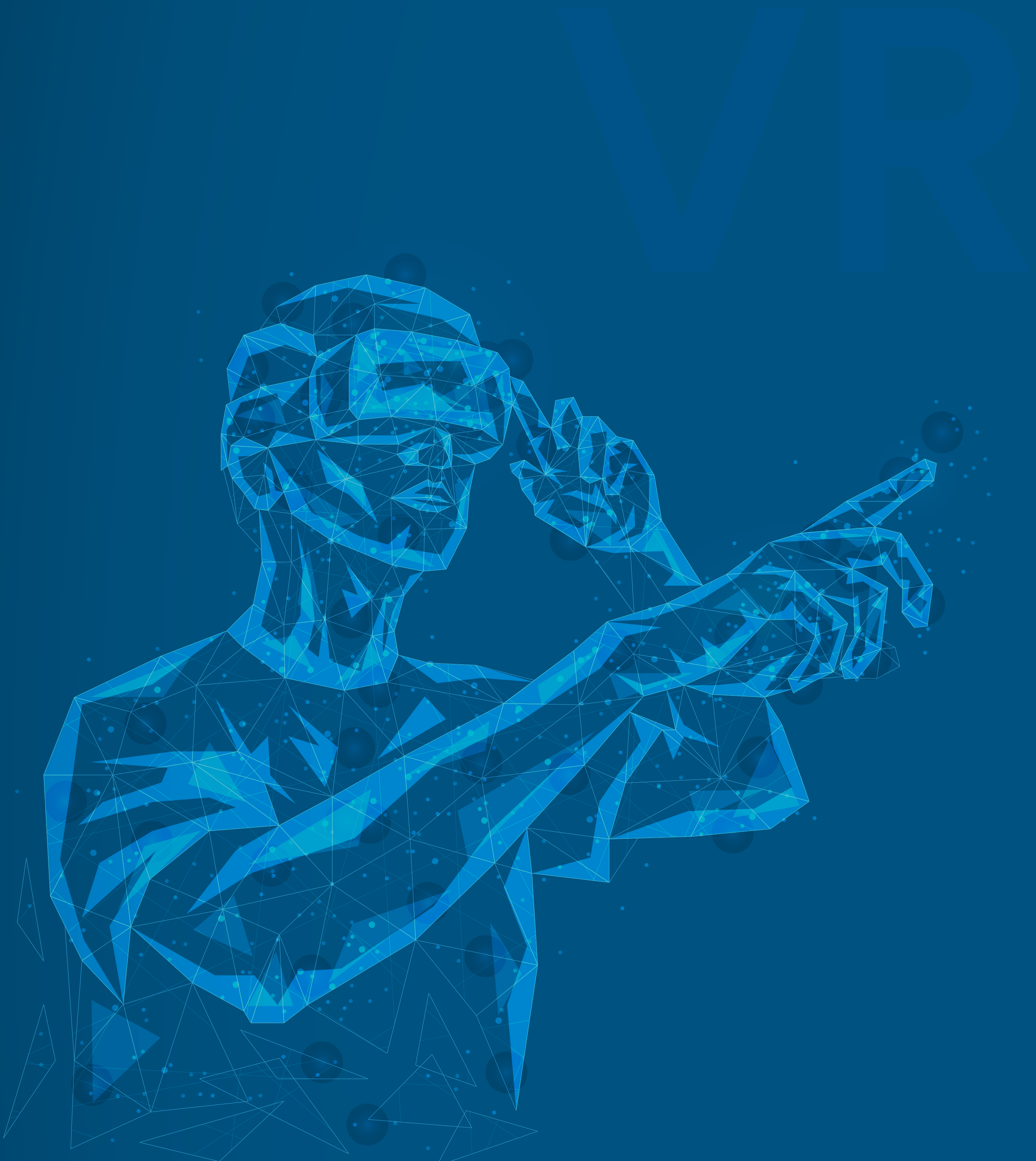
KIRTANE & PANDIT

‘Reality Dawns’ New Frontiers in Data Privacy



- F.C.A., C.I.S.A., D.I.S.A. with 20 years of experience in Information Security, Risk, Governance and Compliance. She is certified for ISO27001, ITIL- Foundation, Data Privacy Lead Assessor- Data Security Council of India.
- Before Joining Kirtane & Pandit , she was a Head of Internal Audit and Chief Information Security Officer (CISO) of Universal Sompo General Insurance Co. Ltd. She was at senior level positions in SBI Life Insurance, ICICI Bank, Tata Motors Finance Ltd.

We place our values, standards and ethics very high, in every work we do !

CA. Bhakti Dalbhide

F.C.A., C.I.S.A., D.I.S.A.

Practice area : IT Security & Risk Management

bhakti.d@kirtanepandit.com

Virtual reality (VR), Augmented reality (AR)

Virtual reality (VR), Augmented reality (AR) are new immersive technologies that create distinct experiences by merging the physical world with digital or simulated reality. They are often used interchangeably but have certain differences. The key difference being "Augment" versus "Virtual"!

Virtual Reality

VR aims to create a fully immersive user experience, replacing physical reality with a digital environment

It immerses users in virtual, digital experiences that can include interactive graphics, sound, haptic feedback, wind, water, and more

To create a virtual environment, VR requires special hardware and headset which rely on stereoscopic displays, spatial audio, and motion-tracking sensors to simulate a "real" experience.

Example

1. Marriott has used VR to enable potential customers to view and tour their properties

2. Ford Motor Company uses VR to design and test cars before making a physical prototype

Augmented Reality

AR layers virtual elements onto real-world environments via smartphones or heads -up displays (HUDs)

AR relies on software that extracts data from visual representations of the physical world to overlay and superimpose computer-generated sensory inputs such as sound, video, and graphics.

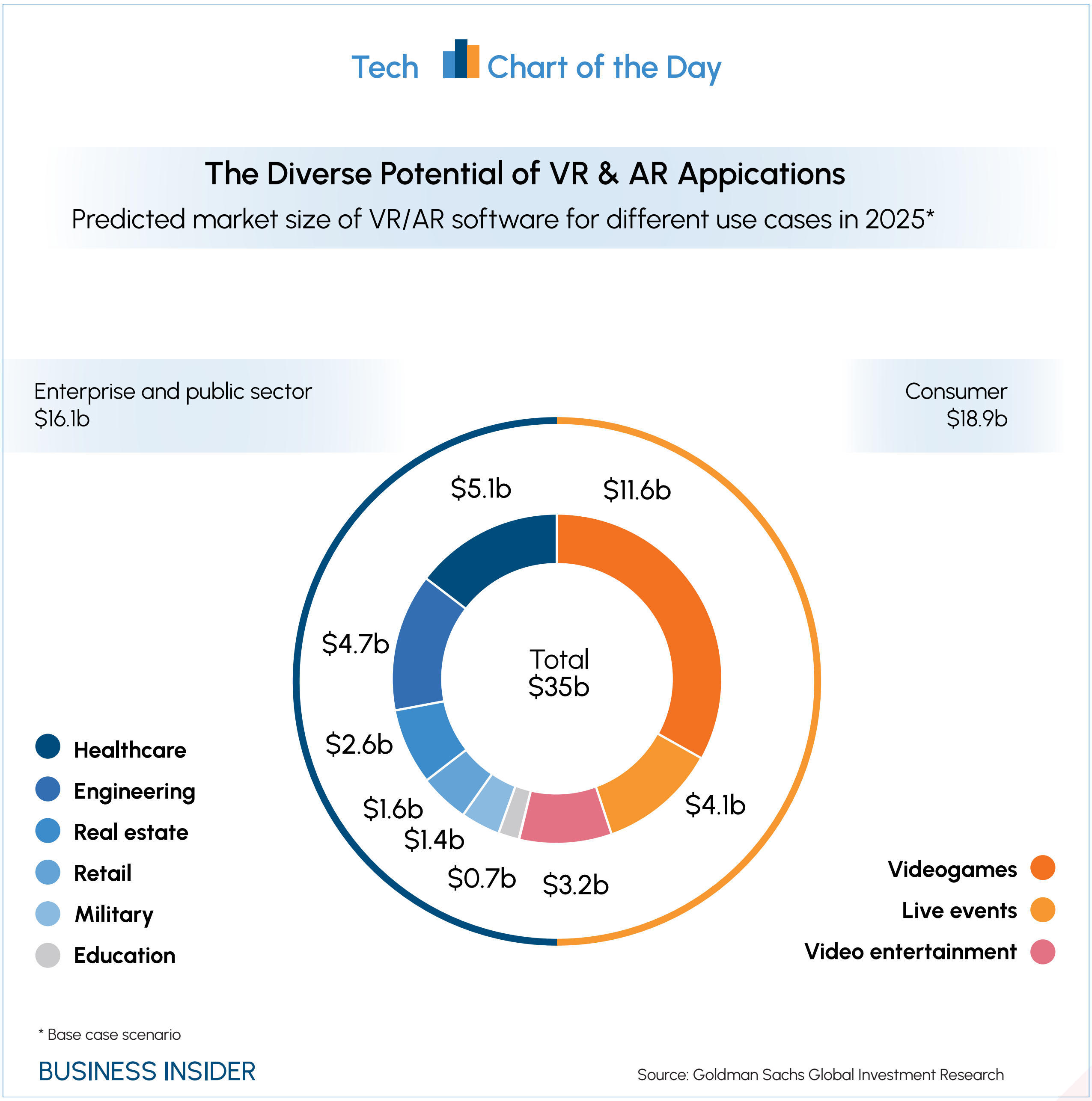
Example

1. Popular game Pokémon Go

2. Ikea, customers can use AR to check whether an item of furniture fits the space in the room.

Immersive technology and Data Collection

Immersive technology is in a nascent stage but the adoption of virtual reality across the globe has been widespread and its potential growth is very clear.



Tech Chart of the Day

The Diverse Potential of VR & AR Appications

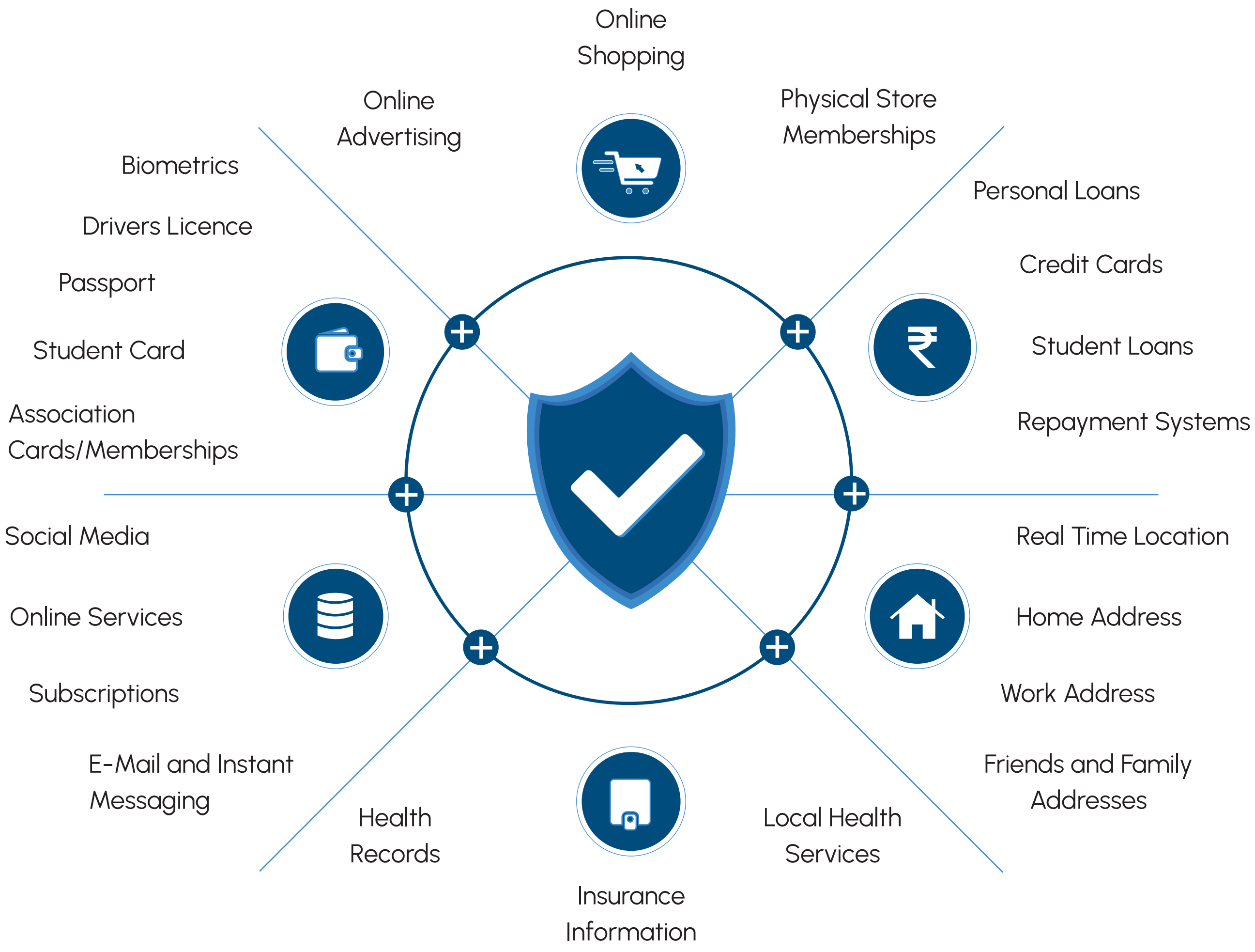
Predicted market size of VR/AR software for different use cases in 2025*

* Base case scenario

BUSINESS INSIDER

Source: Goldman Sachs Global Investment Research

However, this immersive technology cannot function unless it collects a vast amount of data from users that can be classified as personal and sensitive.



Definition of PII

Personal Data includes the name address, Bank Account, Credit card number, passport, DOB, & location data.

Definition of SPD

Sensitive Data includes Financial Data, Health, Data, Sex life, Biometric data, Genetic data, Intersex status, Caste or tribe, Religious belief.

Data Collected by AR/VR Technologies

Pupil dilation, Eye tracking, Gaze, Gait analysis, Body movements, Voice, Fingerprints and IRIS rate.

According to research, Twenty minutes of VR use can generate approximately two million data points and unique recordings of body language.

A detailed understanding of the functioning of AR/ VR throws light on how this immersive technology captures data from the human body, which is beyond the existing definition of Personally Identifiable Information (PII) or Sensitive Personal Data (SPD).

AR/VR technology can identify users with a very high degree of accuracy. Needless to add, if AR/VR systems are compromised, they pose serious dangers to users through the invasion of privacy.

▶ New Technology, New Challenges

Let us review some hypothetical but potentially dangerous scenarios when AR/VR systems are compromised

What if?

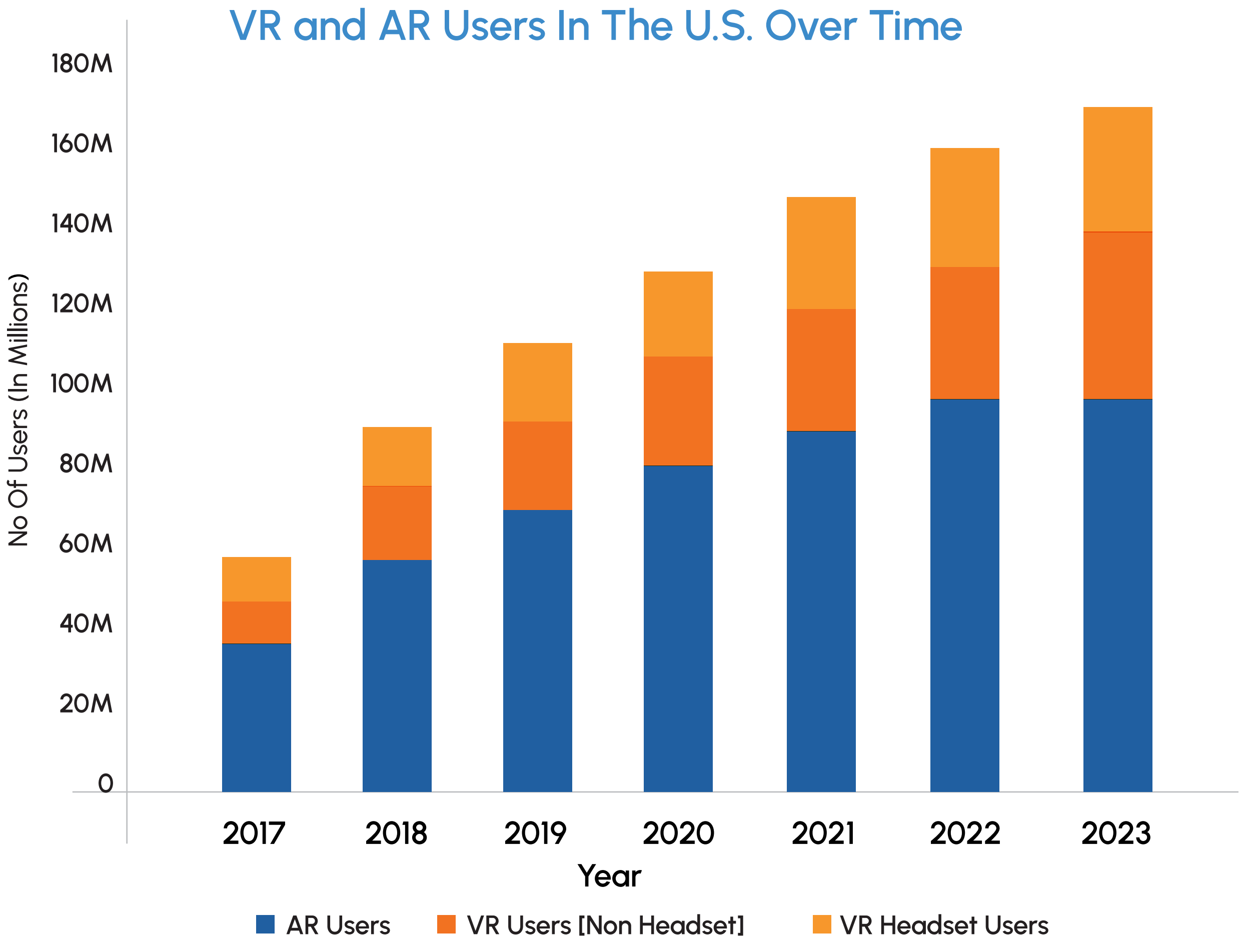
- A doctor monitors patients' vital signs through an AR watch during telerobotic surgery. A compromised AR system can manipulate patient information creating a life-threatening condition for the patient.

- Data collected or leaked from an AR/VR environment can potentially be used to blackmail users for ransom.

- A user is coaxed to walk into a high security zone with help of AR games like Pokemon Go, thereby revealing damaging details about a secure facility.

According to the statistic below, the number of users adopting AR/VR technology in their day-to-day life is growing with time. Just like the present-day dangers of sharing personal information on social media, sharing of the AR/VR data will pose threat, far beyond our current understanding.

US VR and AR Users, 2017-2023



*Source: https://www.zippia.com/advice/virtual-reality-statistics/

What about security?

As with any fast-growing consumer technology, security is typically an afterthought. With the growing adoption of AR/VR technologies, we will soon see challenges similar to when mobile phones became ubiquitous. Bring your Own Device (BYOD) became the buzzword and Enterprises scampered to protect their environments from such devices by introducing Mobile security technology.

End-users

End-user may not be completely aware of the type of data they are sharing while enjoying an immersive technology experience and its subsequent misuse. User education and awareness around the potential dangers of such technology and its misuse will be required.

▶ Enterprises

Enterprises that wish to use this technology would have challenges in protecting the vast amount of personal data collected from these technologies. Enterprises will be required to implement privacy by design and stringent security measures.

▶ Regulators

AR/VR systems were not contemplated by lawmakers while designing many privacy laws. It does not fit directly within existing legal definitions of biometric data. The regulator has to broaden the definition of personally identified information and its protection measures.

We firmly believe that the widespread use and adoption of such technology in Enterprises will pose serious challenges to regulators, law enforcement, and data privacy advocates to define clear laws and regulations around the operational use of such technology.

Organizations will need to maintain their security posture and stay ahead of the curve by adopting new technology.

We also firmly believe that the use of technology and generated data by organizations will have to be audited according to data privacy regulations, standards such as ISO or GDPR.

Enterprise and end-users will be well advised to understand the potential dangers such technologies pose for data privacy, confidentiality, and misuse.

We are always there to help organizations deal with Cybersecurity challenges. Get in touch.

Overview of Kirtane & Pandit LLP

Kirtane & Pandit LLP, Chartered Accountants (KPCA) is an Accounting, Auditing & Consulting firm with a widespread established network of financial experts across India. With the "Step ahead, Always" motto, we partner your growth journey with the delivery of sound financial solutions & value added approach.

With an extensive experience of 65+ years, we deliver a wide range of professional services in the areas of Assurance, Accounting & Advisory to listed & reputed companies from varied industries across the globe.

We are registered members of PCOAB, SEC, US & feature in the A category firm list published by the RBI.

6 decades of Experience

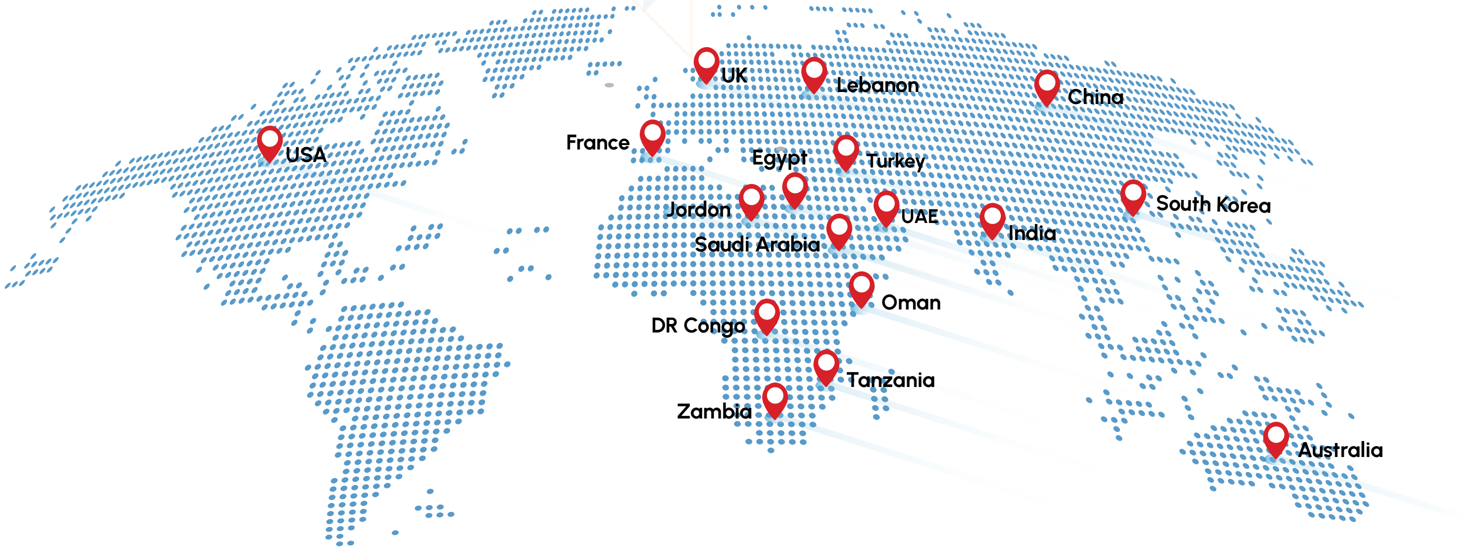
Operating across India with 7 Offices

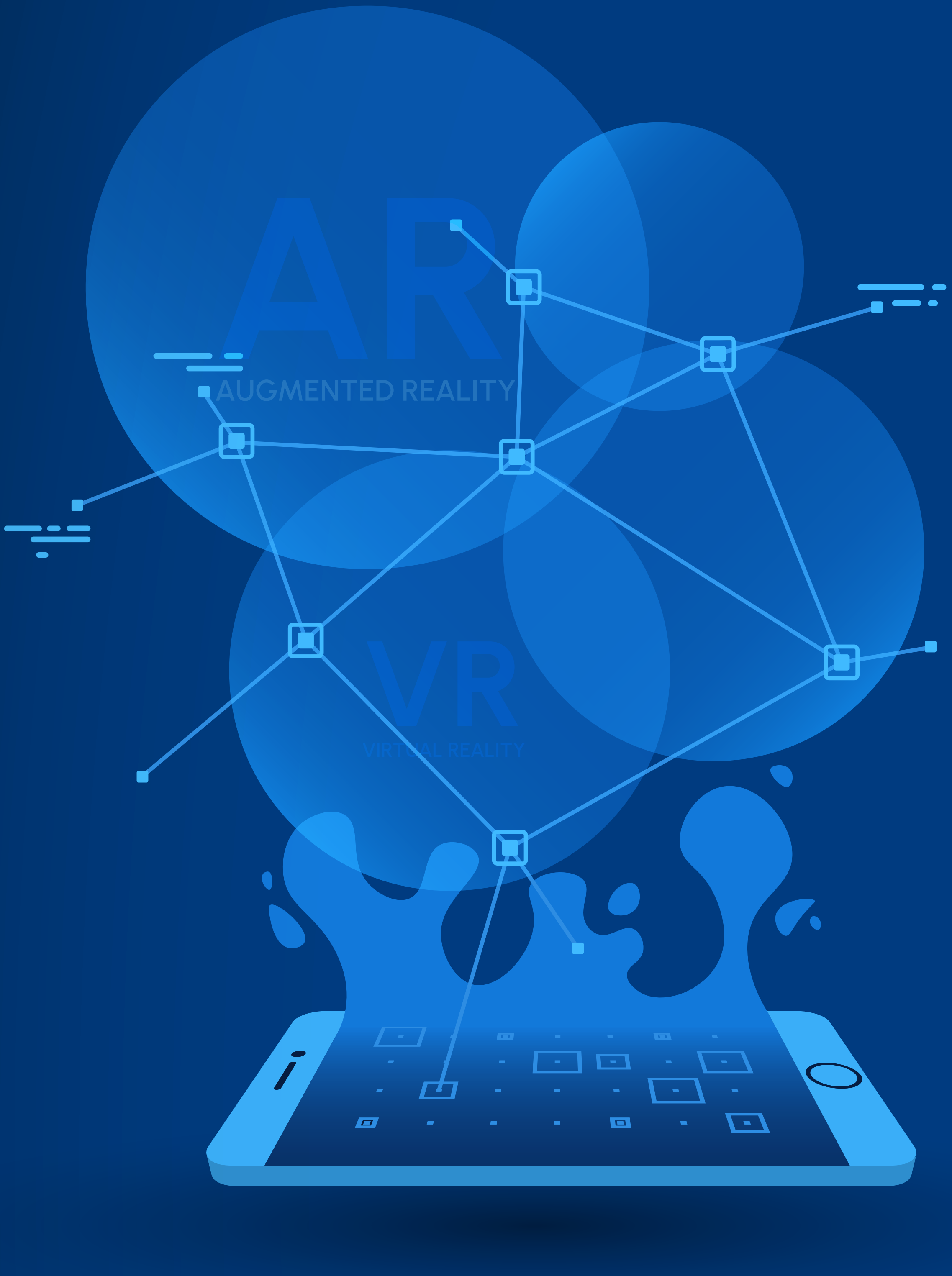
33 Partners

700+ Team of Professionals & experts

Client spread across 30+ Industries

Multinational Clientele parented from 17+ countries





kpca@kirtanepandit.com | www.kirtanepandit.com