Charting the Next Digital Frontier: The IC CDO Perspective

The Future of Intelligence Data in the Age of Immersive Technology and the Metaverse

April 2024

UNITED STATES INTELLIGENCE COMMUNITY
COLLABORATUS
VIRTUS
FIDES

(U) This paper represents insights and recommendations from the IC Chief Data Officer (CDO) generated through a series of collaborative engagements across the private sector, academia, and government to address the data challenges and opportunities presented by immersive technology.

(U) Under the advisement of the Office of General Counsel:

1. The USG is not obligated to act on any comment, input, advice, or recommendation submitted by a participant;
2. There is no expectation of compensation by participants;
3. The USG is not obligated to enter into any kind of contractual relationship with participants by virtue of their participation in this exchange;
4. Participation in this exchange cannot be charged to a USG contract unless participation is required by the contract and approved by the USG Contracting Officer.

(U) Participants may direct feedback about the paper to the Data Future Group who can be reached at IC_CDO_DATA_Exchange@odni.gov.

Charting the Next Digital Frontier: The IC CDO Perspective

The Future of Intelligence Data in the Age of Immersive Technology and the Metaverse

Overview

With predictions that immersive technologies and the next evolution of the Internet may reach maturity by 2028, it is imperative that the Intelligence Community (IC) understand the impacts these new technologies will have on National Security and the future of Intelligence. National Security and IC leaders need to take a collective step back and understand the full scope of these technologies, the impact and opportunities. Current planning, prioritization, and resourcing will ensure the IC is optimized to the fullest extent possible for this future operating mission environment. Predictions and early adoptions are indicating that these technologies and platforms are the place where societal interaction and commerce will increasingly occur. This paper represents insights and recommendations from the IC Chief Data Officer (CDO) generated through a series of collaborative engagements across the private sector, academia, and government to address the data challenges and opportunities presented by immersive technology.

The data volume, types, and way data will be generated and shared and how data ownership will be defined, and the platforms by which they move across become critical to the future of intelligence. Immersive technologies generate data through user and machine interaction with virtual reality (VR), augmented reality (AR), and physical environments. New data types such as VR/AR generated biometric and environmental sensor data, along with near-real time reality data streams will present unique challenges for the IC. For example, a study from Stanford University Virtual Human Interaction, estimates that 20 minutes in a VR simulation results in almost 2 million unique recordings of body language[1]. Furthermore, research highlights that a user can be uniquely identified with almost 95% accuracy with just 276 seconds of VR data[2].

This paper explores how immersive technologies will impact data governance, data security, and data management, as well as how the IC can prepare to meet the challenges and opportunities of a global competitive landscape that is rapidly adopting these new capabilities. Building a comprehensive data environment, for the IC workforce and its partners, requires data solutions and processes to be constructed around a well-formed logical framework.

Motivation

To maintain decision advantage in a world that is increasingly connected between physical and virtual environments, intelligence professionals will need to leverage immersive technologies as

[1] "Protecting Nonverbal Data Tracked in Virtual Reality", Jeremy Bailenson, Stanford University, 2018

[2] "Personal identifiability of user tracking data during observation of 360-degree VR video", Mark Roman Miler, et. al., Stanford University, 2020

they work, learn, and interact. While often thought of as wearable devices, immersive technologies include **VR, AR,** and **Mixed Reality (MR)** capabilities, and extend to a range of other devices and capabilities:

- **Spatial computing** represents hardware devices and software applications that enable people to experience three-dimensional virtual content that is blended with the physical world.
- **Internet of Things (IoT)** devices leverage sensors to provide users with contextual awareness of their physical surroundings.
- **5G/6G** cellular communications networks can provide the bandwidth and speed technology experiences require.
- Cloud services enable **Artificial Intelligence (AI)** and **Machine Learning (ML)** generated realities.

All these capabilities are associated with the concept of a **metaverse**, which is a variety of persistent, connected, and shared virtual worlds in which people interact. Governments, industry, and the academic research community have all made major investments into standing up various versions of a metaverse. This new paradigm of computing with immersive capabilities is seen as the next iteration of the Internet and is driving the exponential growth of the World Wide Web that the IC must adapt to for mission support.

Data Governance in an Evolving Landscape of Immersive Technologies

Immersive technology uses numerous sensors to capture data about a person, physical spaces, and their interactions. These datasets are similar in complexity to DNA data, which can uniquely identify a person. However, IC immersive datasets represent a unique challenge for data governance that defines responsibilities and roles to administer data assets, and data management that defines the development and execution of plans and others to control and protect data assets. These challenges include complex factors such as VR/AR new data types and required algorithms for visualization. These may require updating or developing new approaches to fully leverage, near real-time responses to protect identities and correct data errors.

The goal of IC immersive technology data governance will be to provide the appropriate responsibilities, roles, functions, and practices to effectively manage this data throughout its lifecycle. Governing this data effectively will require legal compliance and policy adherence to enable the IC to maximize the intelligence value of the data while maintaining a high ethical standard.

Partnering closely with data teams in each agency, including legal, compliance, records management, classification, and civil liberties and privacy professionals, will help the IC understand governing authorities. These include legal obligations, information governance responsibilities and best practices for immersive technology data governance.

Data Security and Usage Implications of Immersive Technologies

The IC must enhance current security practices in the areas of monitoring, action evaluation, and data access policy enforcement to ensure immersive data security. Immersive data access control approaches will need to adapt to the dynamics of new data collections. This is critical given that the use of immersive technologies will generate behavioral and biometric data that was previously unavailable, as well as capturing and storing a vast amount of personal data governed by civil liberties and privacy policies.

The IC will need to monitor and respond to legal data protection regulations that govern the collection and use of immersive data. Regulations such as the General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act (CCPA) in the United States can require restrictions on the data produced by immersive hardware and software capabilities. The IC needs to stay engaged and aware that future legal restrictions may have an undesired impact to industry vendors that supply immersive technology to the IC by restricting the type of data generated.

It will be essential for the IC to establish ethical immersive data guidelines that prioritize user data privacy and ensure accountability and transparency in immersive data collection and ethical use practices. This will assist in making data collections consistent with the IC's values and mission, and compliant with legal authorizations.

IC officers at all levels will need to be prepared to recognize and discover the mission value of identifying and sharing actionable intelligence using immersive technology. The digital and data landscape is constantly evolving, and the IC needs to provide programs that strengthen awareness, education, and training to meet today’s data challenges and anticipate the risks and opportunities of tomorrow.

Data Management Impact of Immersive Technologies

With the expected data growth and the need for near-real-time interactions in the immersive technology environment, the IC will need adaptive automated data management capabilities available within each phase of the data lifecycle: data collection, ingestion, protection, processing, dissemination, and disposal. This will require the update of its data management policies as well as consider the adoption of innovative, flexible, scalable, and fast data storage and access solutions.

A key component of required data management plans will be the inclusion of a responsive and automated data quality functions that can support the automated validation, verification, and quality process during data ingestion, collection, and creation activities. This will be critical given that incoming immersive data will require data quality metrics capable of being reported in near real-time for proper data status monitoring.

From Vision to Reality: Data Excellence in a Transforming World

This paper is a call to action for senior leadership across the IC. IC senior leaders have expressed a strong desire to acquire and implement emerging technology to push the boundaries of what is possible for the IC.

The IC has an opportunity to effectively support future mission needs by proactively addressing the complexities of immersive data. The challenge is for the IC to ensure IC immersive data is governed, managed, generated, acquired, ingested, processed, stored, secured, accessed, disseminated, and retained in accordance with all applicable laws and statutes while supporting future immersive mission use cases.

As the IC continues to prioritize data as a strategic and operational asset, it must ensure that the data generated by immersive technologies in conjunction with other capabilities like AI and machine learning are thoroughly evaluated and integrated with data governance and end-to-end data management plans. To maintain decision and intelligence advantage at the speed of mission in a competitive landscape being transformed by immersive and emerging technologies, the IC will need to work together to address all the ways in which the growing volume and complexity of immersive data are demanding change.

Actions To Take Now

The following action items are recommended priorities to completed in the near-term (90-day sprints) or long term (greater than 90 days):

Empower Collaboration & Innovation through Public/Private Partnership through Effective Governance.

- Ensure policy organizations commit to preparing and issuing any new policies for National Security Systems (NSS) with Immersive Technology in mind.
    - Ensure policies align with the future ICD-504, to collaborate with IC CDO to ensure incorporation of legal rights and policy requirements for civil liberties, privacy, and transparency into data management oversight activities. Identify and address issues such as jurisdiction, enforcement of laws, criminal investigations, and cooperation among different legal systems.
    - IC CDO Council members will update their Data Management Plans (DMPs) to include Immersive Technology data so that during implementation, AI is leveraged for automation of Immersive Technology data management within each data life-cycle phase.

Provide Effective Digital Identity Security and Verifiable Management of Immersive Data

- PC/DPI/DFG will collaborate with IC CIO/CSG team and the Zero Trust Steering Committee (ZTSC) to leverage external stakeholders' data security recommendations in the IC Zero Trust Data Pillar documentation and subsequent implementations.
- All IC CDO Council members will maintain immersive technology verified digital identities data consistently across domains.

Engage to Educate about the Criticality of Immersive Technology and the Metaverse for National Security

- Identify and appoint an IC Sponsor to champion activities to coordinate and promote awareness of immersive technologies.
- IC CDO will collaborate with the DoD Chief Digital and Artificial Intelligence Officer (CDAO), private sector, and US Congress to explore and address challenges surrounding virtual identity data, attribution, and return on investment.
- Collaborate with IC stakeholders to support the PDDNI engagements with Congressional offices to provide situational awareness of the critical importance of immersive technologies to the IC mission.
- IC CDO and IC CIO, as part of an immersive technology engagement plan, each need to
- become ongoing active participants in any international standards bodies which may publish standards related to Immersive Technologies.
- Update the IC Data Lexicon to ensure digital literacy and skills development for the use and management of immersive technology data.
- In collaboration with the IC stakeholders, host an Immersive Technology Summit that showcases mission value from across the community for an audience of government, private sector, and academic partners.
- Establish an unclassified immersive technology sandbox to enable collaboration and experimentation mainly between the IC and Industry partners.

April 2024