Into the Metaverse:

TECHNOLOGY, LEGAL IMPLICATIONS & ACTIONS

Karen Silverman, J.D. - The Cantellus Group
Thomas A. Campbell, Ph.D. - FutureGrasp

The Cantellus Group
cantellusgroup.com
Search The Cantellus Group
info@thecantellusgroup.com

FutureGrasp™
futuregrasp.com
Search Future Grasp
info@futuregrasp.com

CONTENTS

About the Authors

Karen Silverman, J.D.

Karen is a leading global expert in practical governance strategies for AI and other frontier technologies. As the CEO and Founder of The Cantellus Group, she advises Fortune 50 companies, startups, consortia, and governments on how to govern cutting-edge technologies in a rapidly changing policy environment. Her expertise is informed by more than 20 years of practice and management leadership at Latham & Watkins, LLP where she advised global businesses in complex antitrust matters, M&A, governance, ESG, and crisis management.

Karen is a World Economic Forum Global Innovator and sits on its Global AI Council where she has contributed to the Board Toolkit for AI and ongoing work on AI, data, and cybersecurity issues. She has been named one of the Top Ten Legal Innovators (The Financial Times, 2019), a Top AI Lawyer in California (California Daily Journal, 2019), and one of the 100 Brilliant Women in AI Ethics (Women in AI Ethics, 2020).

As a leading voice in the governance of AI and other frontier technologies, she is a regular speaker at conferences and forums including CogX, RSA, HIMSS, the Athens Roundtable, National Judicial College, Aspen Institute Technology Fellows and Berkeley Law. Her thoughts on the governance, oversight, and real-world applications of AI, AR, VR, and other nascent technologies are featured in The World Economic Forum's Agenda and the AI Journal.

Karen currently chairs the board of Krunam, a public benefit corporation developing complex content moderation tools, and sits on the Board of Directors and board committees of multiple nonprofits.

Prior to founding The Cantellus Group, Karen spent 20 years at Latham & Watkins, LLP in global strategic and tactical management roles, including Office Managing Partner for the San Francisco office. She specialized in global merger control and helped to build the firm's leading global M&A competition practice. For this work, she has been recognized as a top antitrust practitioner by the GCR, Law 360, Legal 500, Who's Who, the Daily Journal, The Recorder, and SF Business Times. Karen earned her J.D. from the University of California at Berkeley and her B.A. from Wellesley College. She held early career roles at McCutchen LLP, Jones Day LLP, Paul Hastings LLP, the Department of Justice's Antitrust Division, and the Securities and Exchange Commission.

Thomas A. Campbell, Ph.D.

Dr. Campbell is Founder and CEO of FutureGrasp, a global technology advisory group focused on emerging technologies, especially artificial intelligence (AI) and advanced materials, and their trends and implications in geopolitics, national security, and economics.

From 2/2015 to 8/2017, he was the first National Intelligence Officer for Technology (NIO-TECH) with the National Intelligence Council (NIC) in the Office of the Director of National Intelligence (ODNI).

He has informed senior policymakers and corporate leadership, enabled millions of dollars in industry and academic funding, broken ground in multiple new research areas, served as an expert witness in technology-related litigations, and kept diverse groups abreast of the rapid pace and implications of technology change. Dr. Campbell has extensive experience in government, academia, and industry - nationally and internationally.

Dr. Campbell received the prestigious Alexander von Humboldt Research Fellowship for one year of fully funded post-doctoral research in Freiburg, Germany. He performed all his research in the German language.

He holds a Ph.D. in Aerospace Engineering Sciences (funded by a three-year NASA Graduate Student Research Program fellowship) from the University of Colorado at Boulder, and a B.E. in Mechanical Engineering (Magna Cum Laude, with Honors) from Vanderbilt University.

New technologies always yield surprising implications. The Gutenberg printing press made knowledge available to the masses and, unsurprisingly, enabled propaganda and misinformation. Digital platforms are the same, and tools such as artificial intelligence (AI) that drive industry also empower autonomous weapons. As new technologies are released into the mainstream and we try to digest and manage them, our first (and appropriate) instinct is to try to apply existing rules and regulations to establish guardrails and recourse. We can be slow to understand where new technologies are raising genuinely new questions or to conclude that new and more adequate rules may be needed to address those questions.

In the United States, we rely heavily on adversarial litigation to produce working rules that set the boundaries on behaviors and liability. This means that new enforceable standards take a long time to develop and tend to trail the emergence of societal norms and expectations; they often focus on edge cases and are decided by judges and juries with differing levels of technology expertise and under widely differing rules.[1] Legislation may be a more coherent approach to setting rules, but it also is sluggish and will almost always over- or under-regulate, come too soon or too late, and/or produce unnecessary constraints along with necessary ones. Alongside litigation and legislation, as we think about formulating governing rules for AI and other frontier technologies, we need to apply specific foresight and more agile governance now – at the operational level – in business and in government.

[1] Statutes and cases interpreting arise at federal, state, and local levels. In the United States alone, there are over 85,000 different jurisdictions enforcing standards – many of the details of which differ one to the next.

Waiting for the rules of the road to emerge in the usual course will not work for AI generally, and it will especially not work for augmented or virtual reality (AR/VR, aka, XR, "extended reality") applications. For purposes of this article, "VR" or "virtual reality" means a fully immersive and self-contained, digitally-generated environment. Generally, this requires a headset or goggles. "AR" or "augmented reality" denotes digitally-generated content that overlays and/or interacts with the natural world (think Pokémon Go), and may operate through a personal phone, transparent glasses or other technologies installed in the field. The lines between VR and AR are blurry and will become even foggier as these technologies advance. For now, it is worth keeping the distinction in mind for some purposes, while for others they can be treated together as "XR."

Whether in society, business, or government, our time is already filled with screens of all kinds; many people are digitally immersed most waking hours. While on the one hand we can expect almost the full range of known human experience to occur in these digital settings, so too can we anticipate entirely new experiences and capabilities. Individuals will be able to take on a variety of novel forms and to choose very narrowly defined worlds in which to do more and more of their living. Our path into the so-called metaverse – "meta" (beyond) and "verse" (from "universe") – will assuredly lead to unforeseen behavioral, societal, and legal implications.

Unknown is how those experiences will impact individuals and organizations, what sorts of disputes they will produce, and what challenges to social systems warrant consideration. What might be the implications when (very soon) our digital lives are taken to a new level in XR in which it can be difficult to discern what is real and what is computer-generated? Are we psychologically prepared for our digital avatars to act autonomously? What cybersecurity/privacy/ethics risks exist when one's personality and data are uploaded completely? What will controlling platforms do with unprecedented volumes of our identifiable data collected every second of XR use? What legal implications will individuals and companies be forced to reckon with in these complex digital worlds?

Here we review the current state-of-the-art in XR, raise potential legal implications of these next plateaus of digital engagement, and offer ways for industry and government to engage now as they put these technologies to use.

As we stand on the threshold of unprecedented levels of digital immersion, more complex challenges are on the way. We need to turn to these challenges now – and not to enter the metaverse with blinders on. As written in the book Ready Player Two, "And sometimes when you think you've reached the end of the game, suddenly you find yourself standing at the start of a whole new level. A level you've never seen before." We hope this note offers some utility to prepare as we enter the metaverse.

OVERVIEW OF XR STATE-OF-THE-ART

XR technology is evolving fast. A recent review by CNET of the top VR systems demonstrates how far the field has progressed. In their opinion, currently leading the field for affordability and capabilities is Facebook's Oculus Quest 2 system. Other high-end systems include the HP Reverb G2, the Valve Index, the Sony PlayStation VR, and the HTC Vive Cosmos. These systems offer not only visual digital immersion, but also haptic sensors worn on the hands that enable one to detect and grab objects within virtual environments.

Highly capable AR systems are available, too. As wareable.com notes, "[t]hey could add useful 3D information, like emails, directions, instructions or virtual holograms, into your visual field. So you wouldn't need to look down at a screen or away from your loved ones. And you could control your futuristic glasses with simple taps, gestures or your voice. That's the dream of augmented reality – or at least one of them."

A few statistics clarify the potential market impact of the metaverse:

- In 2021, nearly 60 million Americans will use VR applications, and 93.3 million will use AR applications at least once a month.
- Per the Washington Post, "Global spending on AR and VR is expected to jump more than sixfold to $72.8 billion in 2024 from about $12 billion in 2020 as more companies adopt the technology following the pandemic, according to market research firm IDC."

Use cases, both current and potential, run the gamut of social activities. In VR, gaming is especially prominent, as are athletic, medical, military, and empathic training applications. The ability to immerse oneself with a customized avatar has been embraced by millions of players. In addition to visual and haptic controls, one can also use omni-directional treadmills to 'walk' within the virtual environment while physically staying in one place. In AR, the fusion of reality and digital enhancements opens new opportunities in enterprise software, health and fitness, productivity, and wearable sound (to replace earbuds with a more enhanced product also offering video). For example, if one is visiting a new city, one can use digital information overlays in AR to provide historical context or find that perfect restaurant faster.

Today, such XR applications are still laden with reports of awkward and heavy headsets, induced vertigo issues, limiting tethers to a desktop or other system (e.g., the AR glasses under development by Apple will require a hookup to an iPhone), lack of XR software platforms, and concerns about the potential for relentless advertising that can overwhelm the experience. Nevertheless, it won't be long before more comfortable systems with desirable software features become available.

A non-comprehensive set of companies leading the way into the metaverse include Facebook (now Meta), ByteDance, Apple, Microsoft, Clearview AI and Vuzix. Brief snapshots of the activities of these companies follow.

Facebook, a.k.a. Meta.

On October 28, 2021, Facebook rebranded itself into the parent company Meta. This move by CEO Mark Zuckerberg is a strong statement that Facebook wants to be the global leader in the metaverse. As reported in The Verge, "Facebook plans to spend at least $10 billion this year [2021] on Facebook Reality Labs, its metaverse division tasked with creating AR and VR hardware, software, and content." The former CTO of Facebook, Mike Schroepfer, stated earlier in a Wall Street Journal webinar that most of Facebook will be executed within VR (their Oculus Quest 2 or later versions) within only a few years.

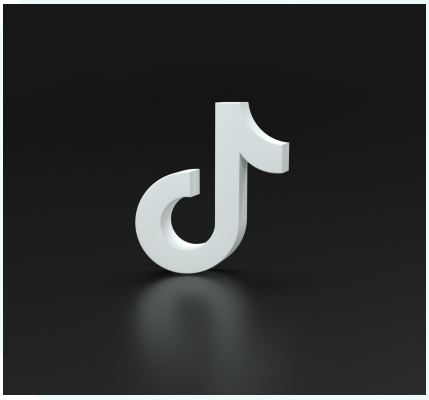
Almost a fifth of Facebook employees worldwide are now working on VR and AR; this equates to roughly 10,000 employees within Facebook's Reality Labs division. Facebook's Oculus Quest 2 (2020) was pre-ordered at five times the rate of Oculus Quest (2019), affirming the increasing popularity of VR. With more than 2.89 billion current users of Facebook, a substantial portion of humanity may soon be routinely active in XR worlds.

Facebook's substantial investment in and desire to move their users into the metaverse have been met with some skepticism over its approach, such as the requirement that Quest 2 headset owners must have Facebook accounts to activate these VR systems (although this might change soon, per Zuckerberg). The issues around walled gardens are complex and include data privacy improvements and risks, hyper-siloing, obscured criminal activity, and the implications of any vendor having access to volumes of highly personal and granular data (where an avatar looks, how it moves, etc.) that all VR users will routinely produce. (Twenty minutes in a VR simulation yields roughly two million recordings of one's unique body language). Such 'live maps' would offer data accumulation with the concomitant ability to control and monetize users' attention and actions in the physical world.

Advertising in a 3D metaverse could become hyper-targeted and integrated, enabling platforms to move well beyond mere pop-up ads present now on 2D screens. This data issue is by no means confined to Facebook, but rather is a feature of XR itself.

Facebook and Ray-Ban recently began selling 'Ray-Ban Stories,' which enable wearers to record photos and videos hands-free by simply saying "Hey Facebook." Facebook's CTO and former leader of the company's XR division, Andrew Bosworth, told *The Verge* that the purpose of the smart glasses is to "lay the groundwork in the minds of consumers for the many, many, future products that we have to come in this space." Thus, while XR and facial recognition are absent from Ray-Ban Stories, this collaboration signals a broader push to normalize a culture wherein members of the public are always wearing a camera – laying the groundwork for the metaverse. Within days of Facebook's announcement, the Irish DPC and Italian Data Protection Regulator, the Garante, issued a statement questioning whether the smart glasses' small LED indicator light sufficiently notifies passersby when a recording is in progress, thus allowing them to exercise their privacy rights. As a result, European regulators are urging Facebook to launch a public information campaign on how Ray-Ban Stories might lead to the "less obvious recording of their images." Facebook says it plans to work closely with its regulatory partners, in part to "help people understand more about how this new technology works, and the controls they have."

ByteDance.



Posing a technology and commercial challenge to Facebook's Oculus is the recent acquisition of Pico by ByteDance, owner of the most downloaded social media application in the world, TikTok: "With Pico finding its home now at ByteDance, two of the world's largest virtual reality brands now reside inside social media companies."

Apple.

Like Facebook, Apple is also testing its hand in the consumer XR wearables market. Apple Glass, expected to launch in 2022, will function much like the Apple Watch, but with visual displays and AR content - "like arrows overlaid on the street ahead of you to indicate Apple Maps directions." Based on a patent application granted in June 2021, some speculate that Apple is working to differentiate itself from Google Glass and the many issues associated with the product, such as being banned from movie theatres.

As the patent reads, "The modular accessory would also make it possible for venues such as bars and theaters to ban the modular accessory while still allowing the HMD frame (without the accessory) into the venues." Apple developers appear interested in confronting privacy concerns, at least in an initial way, including by giving notice to bystanders when nearby users are recording photos and videos.

Likewise expected in 2022 is Apple's VR/AR headset, which is forecasted to outshine Facebook's Oculus Quest in terms of design and user comfort. A February report from *The Information* notes that the headset will be "equipped with more than a dozen cameras for tracking hand movements in addition to cameras for seeing the outside world, and the design blocks out peripheral vision to prevent light from leaking into the wearer's field of view."

Apple's acquisition of eight (and counting) XR companies over the last several years offers a glimpse into where it sees itself contributing to the metaverse, and where the pitfalls lie. Example acquisitions include Flyby Media, which offers a software application allowing users to leave messages on real-life locations and objects; Emotient, which captures and assesses emotions by reading facial expressions; and Faceshift, which creates animated avatars and other figures that capture a person's facial expressions in real time.

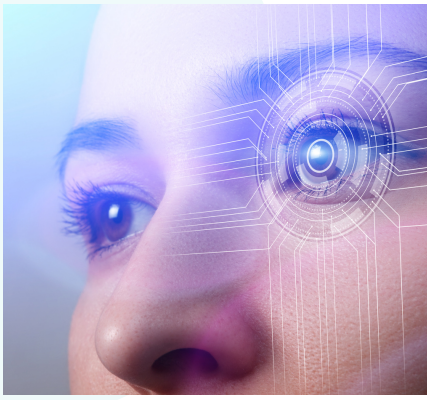
Microsoft.

In the AR community, Microsoft offers one of the most advanced systems: the HoloLens. Of special interest to the US military, the HoloLens is now used by US warfighters. A close collaboration between Microsoft and the US Army is enabling soldier input and feedback, informing iterative design and development. Benefits to the warfighter of having an AR system enhancing their performance include rehearsing and training with realistic simulations, as well as enhanced emotional and tactical preparedness:

"The devices, using what is called the Integrated Visual Augmentation System (IVAS), will allow soldiers to see through smoke and around corners, use holographic imagery for training and have 3D terrain maps projected onto their field of vision at the click of a button…The device represents a paradigm shift for the Army, both in the way it was developed and what it will enable soldiers to do. Instead of planning missions with terrain models cobbled together with boxes, sticks, rocks and other improvised materials, IVAS enables soldiers to use 3D maps depicting the places they will be…Under the new contract, which could be worth up to $21.88 billion, Microsoft will initially produce more than 120,000 headsets for soldiers at a Silicon Valley manufacturing facility. The five-year agreement can be extended for another five years. The devices will first be used by soldiers on foot, and the Army is also conducting experiments with using IVAS in military vehicles so soldiers can see what's around them before stepping outside."

The HoloLens is also being used by NASA as part of its T2 Augmented Reality (T2AR) project, whereby astronauts are using the headshot to "inspect and maintain scientific and exercise equipment." In early September, Microsoft and NASA announced that the HoloLens will soon be used to assist astronauts repairing the International Space Station.

Clearview AI and Vuzix.



Partnerships between facial recognition and wearable display technology companies have raised the first versions of serious concerns around privacy, data tracking, stalking, violence, and crime. For example, Clearview AI & Vuzix are confirmed to soon offer live facial recognition. Clearview has been named in at least eleven lawsuits alleging that it scrapes and sells an extensive image database to law enforcement agencies and private companies without users' consent.

Such advancements and diverse applications bring us to our core question – what legal implications might arise when a large percentage of individuals, corporations, and governments spend much of their time in metaverse communities as a near-routine feature of daily life and/or business operations?

LEGAL IMPLICATIONS

As noted above, litigation and legislation are the two most common ways that enforceable rules are established. Beyond their limitations, it is also important to recognize that we regularly expect much more expansive legal protections than we get. In the United States, most conduct is unregulated and most affirmative 'rights' are enumerated and quite narrow. This gulf – between what the public expects and what the law actually does – is easily spotted in the frustrated and mounting calls for more expansive use of the antitrust laws to "break up" the big tech platforms, although those laws (as written) for the most part don't actually do that.[2]

Likewise, we see it in calls to curb stalking, public corruption, and the spates of untrue, hateful, and harassing speech (often directly threatening women) online. Repeatedly, we learn that our justice system – public or private — is generally not built to regulate offending conduct unless that conduct results in physical or financial harm.

[2] It is reasonable to question whether those platforms (or anyone) should be able to operate in certain ways that affect others, or even be free of regulation. Antitrust is just a perilous way to go about setting industrial policy and can risk doing more harm than good.

While there are some examples of new laws that have become useful to address some online behaviors, such as prohibitions on revenge porn and content that sexually exploits children, in the main the law is appropriately cautious about regulating conduct and speech.

In short, we are regularly surprised to learn just how much behavior and disputes in the natural world are truly governed through norms and manners and a sense of social contract, more than through constitutional rights, criminal laws, civil laws, enabling and administrative regulations or rulemaking. ***If our experience with the internet or political discourse generally is any indication, relying on norms and manners to govern our XR experiences will be entirely inadequate.***

That said, it is mostly too soon to say how existing norms or laws map on to AR and VR, and where specifically we will need new laws (or law enforcement mechanisms). AR, by definition, engages humans in the natural world, so that its consequences may prove to correlate with existing rules more closely. In contrast, in VR the experience is more fully immersive and self-contained, so that impacts and disputes may quickly take on entirely new dimensions. To be sure, AR and VR will share some challenges, but they will also differ.

As we think about what will govern metaverse experiences, we should assume that all the behaviors, assets, and disputes that we encounter in the natural world also will take place in AR and VR, as well as new dimensions and capabilities (automated profiling! flying! transforming! invisibility!). This provokes many questions; below are just a few important ones. We explore some key questions here, but purposefully leave the discussion open-ended to start a dialogue and engagement.

Is the conduct occurring in a private platform 'world' or really in public?

Behavior in the town square is genuinely public and governed by municipal rules and regulations, subject to both public and private enforcement. In contrast, most online behavior occurs on private platforms – albeit widely broadcast – and is largely governed by contracts (often terms of use) between the platform provider and the user or supplier. Contracts are a very useful tool for this, as they can be tailored for specific conditions, negotiable, and contextual. They also are limited however, as a tool for governing pseudo-public activity.

First, there are dramatic asymmetries between the negotiating power of the platform and any single user or vendor. Second, a breach of contract, in the eyes of the law anyway, is not a moral concern, and the remedy for a breach is money damages and/or denial of access to a product or service. Whereas other sorts of claims (such as intentional infliction of harm, civil rights violations, and fraud) may carry more moral weight, contracts generally do not. Thus, it is an interesting question whether contracts – fundamentally a commercial tool – are an appropriate mechanism for governing a full range of behaviors in a virtual world. The answer will differ of course, depending on which behaviors and how effectively participants can meaningfully understand, accept, or reject the terms of an agreement.

A few more issues:

- 1. **Enforcement.** To enforce contract rights and redress a breach, a plaintiff needs to be able to bring a defendant into court in a particular jurisdiction, produce evidence sufficient to persuade a trier of fact, and demonstrate specific harm to that plaintiff (and the quantity of harm). This is a high burden and costly. As we see with privacy claims and every Twitter dispute, it may not be reasonable to expect one user of a virtual platform to enforce their contract rights against another user; likewise it is unclear that it necessarily makes more sense to look to the platform provider to police activity.

- 2. **Constitutional protected-speech complexity.** Not all online activities are constitutionally-protected. Whether or not desirable, inflated assumptions about the scope of protected speech completely muddle the legal basis for setting up rules and enforcing rules for online conduct. This is yet another example of our beliefs dramatically outpacing reality.

- 3. **Constitutional rights and consents complexity**. Is it possible to subject all behaviors to terms of use? Is it possible to fashion adequate consents for specific behaviors? What does that mean in the context of a virtual environment where users may seek out unusual or novel experiences? Which categories of user or platform behaviors go beyond contract, for which the state law enforcement (civil or criminal) is appropriate? How and when - practically – will real world law enforcement address issues occurring entirely in a virtual world? What if those behaviors inflict real psychological harms? Or cause impacts in the real world?

- 4. **Liability and causation.** How do we establish causation in a virtual world or between the virtual world and the real one? When does a virtual world become real? When is the platform itself responsible? Are there certain behaviors for which platform liability cannot be contracted away? Can a platform indemnify users for their behavior, or the behavior of others on the platforms? Can liability be joint and several as between platforms or platforms and users?

- 5. **Agency.** As avatars and AI agents become more autonomous, questions of agency will crop up. This may start as a causation discussion, but it won't end there.

- 6. **Jurisdiction.** Where does activity in a virtual world take place, and which courts and/or law enforcement agencies have authority? How will we resolve jurisdictional conflicts and honor (or not) forum selection clauses? Will traditional choice of law provisions work in this context? Will society need wholly new law enforcement and/or courts to address legal XR issues?

- 7. **Evidence**. What is the value of evidence gathered from XR environments? Is evidence of a user's activation of AR probative of distraction? Are criminal activity or breaches of contracts in a VR environment ever probative in assessing responsibility for real-world behaviors? How will hearsay rules apply to statements in VR? How will we identify or treat synthetic content from an evidentiary perspective?

- 8. **Remedies**. How will we fashion redress? More and more, harms and breaches will be difficult to prove or to scale. Are economic relief or damages adequate? Are the alternatives of injunctive relief (e.g., banning from a platform) or conduct restraints realistic or sufficient? How is that relief going to be fashioned, let alone enforced (and by whom)?

- 9. **Cybersecurity**. The volumes of data generated by AR and VR systems will be substantial. Moreover, the potential for cyber attack vectors goes up exponentially when one is fully immersed digitally with video, audio, and tactile sensors being continuously engaged by users. Will such data be protected by the platforms, or will the onus fall upon the users? If leaks or ransomware attacks occur, who will be held responsible? How will the metaverse be protected from amplified cyber attacks? What legal controls, new regulations, and new laws should be considered to protect metaverse users and platforms?

- 10. **Metaverse Fracturing**. In recent years the internet has seen increasing fracturing across borders, with internet access being intentionally compromised or tightly controlled by several nation states. For example, China imposes its "Great Firewall," in which it blocks access to Western companies such as Facebook and Google to drive traffic toward Chinese alternates such as Baidu and Tencent. We can fully expect that there will be a more expansive 'splinternet' within the metaverse. Senior policymakers and companies need to anticipate how this might play out in the context of limited global metaverse access, and complex legal implications of platforms being blocked across physical and metaverse borders. This issue also gets into the realm of national security that would require a whole separate article.

For crimes and torts, many of the same issues will arise, further complicated by:

- Differences in which enforcement agencies have authority.
- How to account for real harms that occur in virtual environments (the one where the conduct occurs or a different one)?
- How to account for conduct that occurs virtually but for which harms occur in the natural world?
- How to assess the evidentiary value of VR statements and conduct, and whether they can be used to establish patterns, intent, or character?
- How to handle intellectual property? Wealth creation/loss? Inheritance? Taxes? Insurance? Defamation?
- Unauthorized uses or modifications of likeness vs. fair use.
- Surreptitious behaviors that are detected if at all, after the fact.
- Are certain human rights required to be observed in VR?
- Rules for children and other vulnerable groups (or are we all vulnerable, given the capabilities of the technologies)?
- How to handle the protection and limits on derivative uses of truly vast quantities of personal data that will be generated every moment by XR, data that can easily be used to identify users?

These and additional questions will present huge challenges to our legal system, and before that, to society, as we encounter behaviors and outcomes that we don't like and for which there may not be any adequate redress in the courts.

ACTION PLAN

Industry and government need to prepare for the metaverse, and so does society. We propose below a few preliminary recommendations to get started. In reality, this work will take time and evolve, and every one of us, as individuals and in our organizations, will have to confront what these developments mean and how to start adjusting to online worlds only limited by our imagination.

1. Accept that XR is different than other technologies and deserves special thought and consideration.

2. Establish clear lines of accountability for development and use of XR in any setting.

3. Involve diverse inputs and perspectives in the design of XR products and use cases.

4. Incorporate safety, security, and boundary conditions by design, building in time and resources to improve product quality and reliability for impacted communities.

5. Adopt agile internal governance practices that can identify and adjust to developing technologies and realities.

6. Study how XR technologies are being used and managed in other parts of industry and government to assess best practices.

7. Engage in discussion around rule-making and regulation, whether you are in private or public organizations.

8. Incorporate XR into board-level and C-level strategy and risk assessments.

9. Communicate with customers and employees about standards and expectations.

10. Be willing to take a breath, leap in thoughtfully, and be prepared for lots of surprises.

CONCLUSION

Whatever form the metaverse takes, and however industry and government engage within it, will reveal itself over time. Nascent versions and applications with XR technologies already exist though, and their breadth and scope will only increase as public appetite and intrigue grows, greater profits become realizable, and the technologies improve. It is crucial to consider and prepare now for this next level of digital immersion.

COMPANY PROFILE

The Cantellus Group

Helps organizations and their leaders better understand – and then better manage – their use of frontier technologies. We deliver the insights and practical approach to guide the direction and decisions that will determine whether (or not) AI tools will correspond with an organization's missions, values, strategies and risk tolerances. We integrate the disciplinary expertise of our advisors, whose backgrounds span law, compliance, government, procurement, medicine, tech, retail, finance and academia. TCG's practical and stakeholder-inclusive approach enables organizations to do better, and then to communicate how and why they are doing better, for customers, employers, regulators and investors.

FutureGrasp

Enables its clients to lead in times of rapid technology change. FutureGrasp team members have worked directly at and with clients in the highest levels in the US Government (White House, National Security Council, Pentagon, Embassies around the world), NATO, INTERPOL, the European Commission, the United Nations, Fortune 500, Silicon Valley venture capital, and startups. Clients rely on us to look beyond the chatter and hype surrounding a new technology and to pragmatically assess the worth and implications of a given path of technological development. Ours is a proven and demonstrated approach that has resulted in accurate forecasting in numerous sectors (artificial intelligence, quantum computing, semiconductors, AR/VR, nanotechnology, cybersecurity, 3D-/4D- printing, energy, and sensitive and dual-use nuclear materials), and expert briefs on their implications. We are especially well-positioned to offer a range of bespoke services for corporate and government clients, including written thought products, expert briefs, expert witnessing in technology-related litigations, startup scaling insights, government and investor connections, and organization and facilitation of roundtables and workshops.

Contact Us

The Cantellus Group

cantellusgroup.com

info@thecantellusgroup.com

Search The Cantellus Group

Future Grasp

futuregrasp.com

info@futuregrasp.com

Search Future Grasp