Maverick* Research: Deepfakes Will Kill the Metaverse; Synthetic Media Could Save It

Published 15 November 2021 - ID G00760389 - 25 min read

By Analyst(s): Darin Stewart

Initiatives: Technology Innovation; CIO Leadership of Innovation, Disruptive Trends and Emerging Practices

> Deepfakes are disrupting and diminishing the digital economy. The damage they cause will worsen as the internet evolves into an immersive metaverse. A trusted ecosystem based on blockchain authentication and AI-based detection must be established if synthetic media is to displace deepfakes.

Overview

Specific Maverick Caution

This is "Maverick" research, designed to spark new, unconventional insights. Maverick research is unconstrained by our typical broad consensus-formation process to deliver breakthrough, innovative and disruptive ideas from our research incubator. We are publishing a collection of several Maverick research lines this year, all designed for maximum value and impact. We'll explore each of these lines of research to help you be ahead of the mainstream and take advantage of trends and insights that could impact your IT strategy and your organization (see Note 1).

This note is the third installment in a Maverick series on disinformation including Welcome to the Splinternet — How Internet Fragmentation Disrupts Business and Threatens Society and How Disinformation Is Destroying Business and How to Fight Back.

Maverick Findings

- Deepfake media is moving from the darker corners of the web to take center stage in every arena. This is undermining trust to the point that the digital economy as a whole is in jeopardy. This risk will grow exponentially as the internet evolves into an immersive metaverse.
- Legitimate synthetic media are different from illicit deepfakes, even though they utilize the same underlying technologies. This distinction is essential to ensuring that the potential of synthetic media is not overshadowed by deepfakes, to the point that their useful application is no longer possible and their full potential cannot be realized.
- Digital humans, synthetic avatars, agents and environments are already commonplace and will be ubiquitous in the metaverse. This requires a trusted and verifiable environment if the digital economy is to thrive. At this point, such an environment does not exist.
- Both deepfake detection and ubiquitous synthetic media authentication are necessary to create and preserve a trusted online environment. Blockchain is emerging as the key to creating this ecosystem, but is being adopted too slowly to ensure the digital economy is preserved and a trustworthy metaverse is ushered in.

Maverick Recommendations

IT leaders and CIOs planning to defend against and respond to disinformation should:

- Begin utilizing digital humans in corporate communications and customer interactions. This includes artificial reality identities (ARIs) for client interactions, content localization with digital humans and environments, and avatar-augmented chatbots, among other applications
- Encode all published content with “tamper-evident” metadata provided by or registered with a blockchain-based authentication and validation service. Do not purchase or accept content that does not carry this tamper-evident authentication and provenance information.
- Do not utilize or patronize any service or platform that promotes, boosts or monetizes content that is not validated and verified with unalterable provenance data.

- Take precautions against deepfake attacks, up to and including banking synthetic models of public figures. Invest in detection and reaction tools and strategies proactively, so as to be prepared for attacks and disinformation campaigns. Actively scrutinize content with deepfake detection mechanisms. Publicize any manipulated media discovered in this process.

Maverick Research

This is "Maverick" research, designed to spark new, unconventional insights. Maverick research is unconstrained by our typical broad consensus-formation process to deliver breakthrough, innovative and disruptive ideas from our research incubator. We are publishing a collection of several Maverick research lines this year, all designed for maximum value and impact. We'll explore each of these lines of research to help you be ahead of the mainstream and take advantage of trends and insights that could impact your IT strategy and your organization (see Note 1).

Analysis

The future will be fake. It is time to reconcile with this inevitability and learn to adapt. Synthetic media, better known as “deepfakes,” are moving from the darker corners of the web to take center stage on social media, advertising and even corporate communications. The cost and complexity of the tools and skills necessary to create quality synthetic media are plummeting. At the same time the availability of these tools and the quality of their product are improving exponentially. In many cases, deepfaked images, audio and video are indistinguishable from authentic media. This is rapidly becoming the rule rather than the exception. When anyone can create a high-quality fake on their iPhone or hire a deepfake professional on fiverr, pervasive synthetic media is inevitable. This will either result in the death of the web as a useful platform, or the inauguration of a new metaverse of legitimate applications and opportunities.

To date, the most common applications of deepfake technologies have been less than laudable. Between 90% and 95% of synthetic media available on the web is nonconsensual pornography. [1] Manipulated videos of politicians and public officials are standard campaign collateral. [2] PR firms specializing in disinformation are available to create and promote whatever reality their clients are willing to pay for. These trends do not bode well for the future of a “free and open internet.”

At the same time, synthetic media enables new capabilities that are beneficial to both the producer and consumer. In October 2020, soccer legend David Beckham appeared in a video for the Malaria Must Die Campaign to raise both awareness and funding to end the disease. In the video, Beckham speaks nine different languages fluently. At the end of the short film, Beckham ages 30 years to speak from the future, announcing the eradication of malaria. The video enabled the sports superstar to speak directly to the people most impacted by the disease, and to do so in their own language.

Beckham is not a polyglot. Nor is he a time traveler. Both of these feats were accomplished with a commercially available synthetic media production tool. [3] Similar feats are occurring in a corporate setting. To demonstrate the capabilities of its Omniverse platform, NVIDIA inserted 14 seconds of fully synthetic footage of CEO Jensen Huang into his Keynote address during the GTC 2021 conference. [4] No one noticed the segment was fake until NVIDIA revealed the switch and reveled in the positive press coverage.

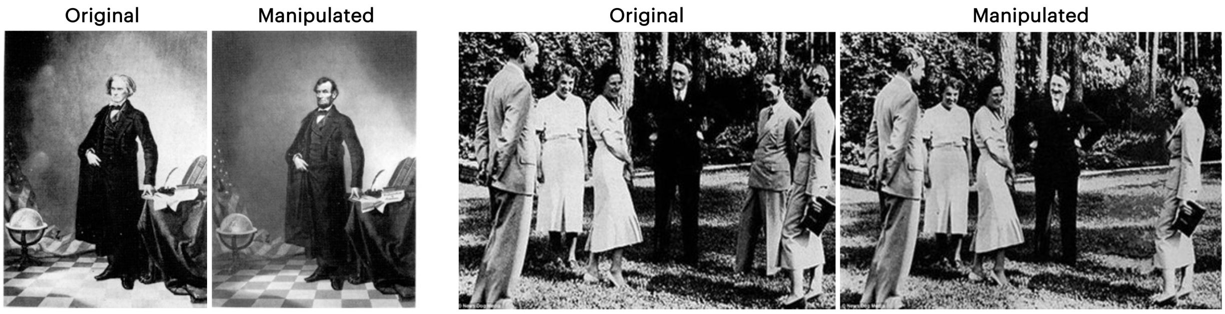
Most new and disruptive technologies flirt with the unethical side of their markets. The ubiquitous and unmoderated nature of the internet only amplifies this tendency. The ultimate fate of those technologies, becoming mechanisms for positive ends or tools for more nefarious objectives, depends on the attitudes and actions of the participants in that marketplace. Developers, vendors, users and even regulators must all cooperate and, in many cases, coordinate to guide an emerging technology toward a worthwhile outcome.

Synthetic media is approaching a crossroads. With appropriate attention and guidance, these technologies can be shaped to enable a more open and capable internet, potentially ushering in the long-promised immersive and inclusive metaverse. [5] Without intentional and coordinated guidance, deepfakes will continue along their current trajectory of deceitful manipulation and salacious prurience with no legitimate utility to anyone.

Distinguishing Deepfakes From Synthetic Media

Manipulated media has been with us for a very long time. In around 1860, the head of Abraham Lincoln was superimposed on the body of James Calhoun to give Lincoln a more presidential bearing. In a particularly ironic case in 1937, Nazi Minister of Propaganda Joseph Goebbels was edited out of an official party photo when he incurred the displeasure of Adolf Hitler (see Figure 1). [6] Deepfakes are nothing new. They are now just more convincing.

Figure 1. Early Political Media Manipulation



Source: United States Library of Congress, Prints & Photographs Division

Instead of photo negatives and scissors, the latest incarnation of synthetic media relies on generative AI, specifically generative adversarial networks (GANs). In essence, two AIs, one creating fake media and one trying to detect fake media, compete until the detecting AI can no longer tell fact from fake. The technique first emerged into the public space in 2017 on the social media service Reddit. A redditor named “deepfakes” was face-swapping celebrities with pornographic performers and sharing the mashups with his ever-growing group of fans and followers. [7] Like many other brand names that have become generically associated with common products (Scotch tape, Band-Aids, etc.), the name “deepfake” transferred from the person to the technique, which he freely shared online.

“Deepfake” and “synthetic media” are not synonyms. Deepfakes are not suitable for legitimate purposes. Synthetic media have nearly unlimited potential for beneficial applications. Developers, vendors and consumers should use these terms correctly and consistently.

The term “Deepfake” is commonly used to describe any media generated or manipulated by AI. It is often used interchangeably with the broader and more accurate label “synthetic media.” Drawing a distinction between the two terms is essential. “Deepfake” originated in association with disreputable uses, and that is where it should stay. Conflating “deepfakes” and “synthetic media” gives the former an air of legitimacy, while causing the latter to become tainted and suspect. Developers, vendors and users should use these terms correctly and consistently. Deepfakes are not suitable for legitimate purposes. Synthetic media have nearly unlimited potential for beneficial applications. It may seem a trivial distinction, a matter of semantics, but in an age of misinformation and conspiracy theory it is essential if the beneficial uses of synthetic media are to survive and thrive.

Putting Synthetic Media to Good Use

David Beckham’s multilingual public service announcement illustrates several potential applications of synthetic media to legitimate business ends. First, rather than clumsy and expensive voiceovers performed by actors in the target language, AI-generated speech can adapt foreign language text to a person’s own voice. [8] Similarly, generative AI can synchronize the movement of their mouth and other facial features to the foreign voice. This results in a natural-looking video, rather than a poorly-dubbed afterthought.

Synthetic media here avoids the disadvantages of both dubbing and subtitling. The presenter’s original performance is preserved, along with their natural expressions, both vocal and physical. This eliminates the distractions caused by out-of-sync audio and visuals. No content is lost to the unavoidable simplification required for subtitling. [9] Beyond these qualitative aspects, it is much cheaper to generate multiple synthetic voice tracks than to hire and record multiple performers for multiple languages. Why shoot video at multiple locations when you can generate multiple environments? The kitchen setting of the NVIDIA keynote was entirely AI-generated.

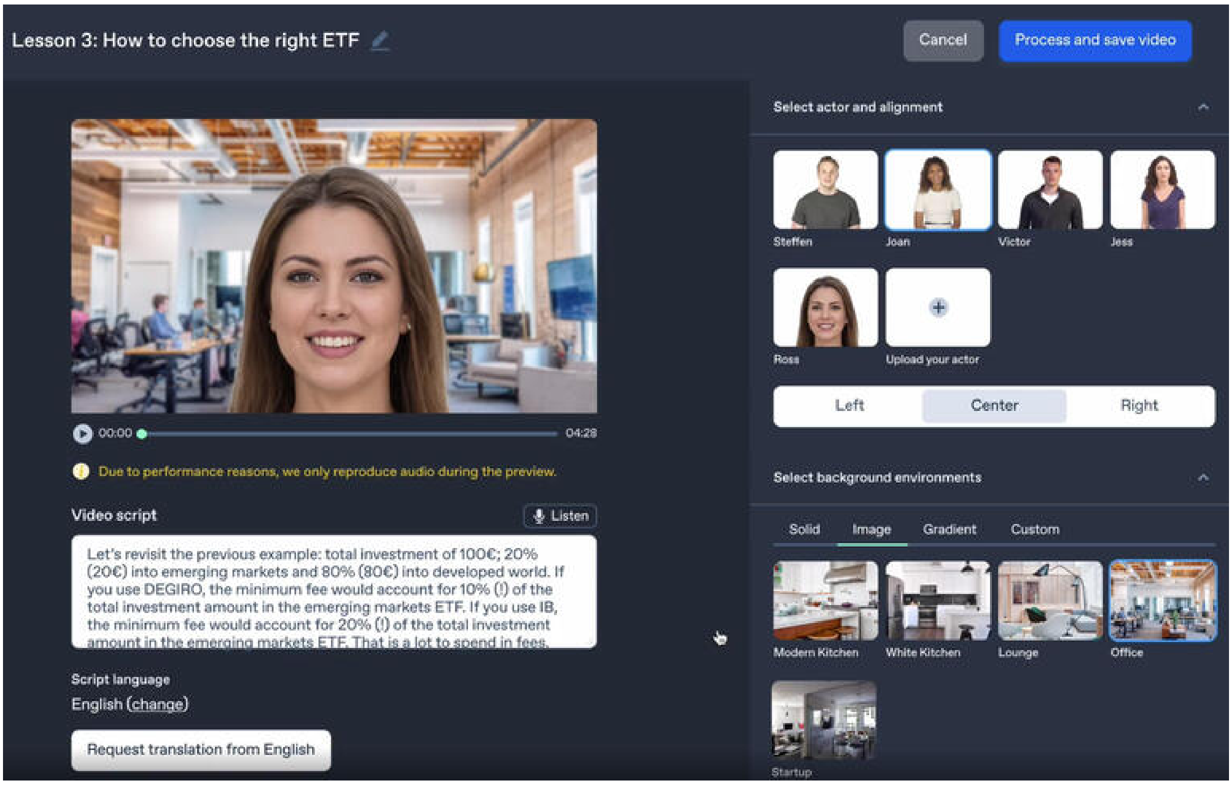
Synthetic media techniques are already in much broader use than is generally known. Synthetic media enabled deceased culinary star Anthony Bourdain to read from his own writings in a film about his life created four years after his death. [10] ESPN hired deepfake artist Shamook to insert deceased team owner Al Davis and NFL Commissioner Pete Rozelle into the documentary “Al Davis vs. The NFL.” [11] Synthetic media is a staple of visual and audio effects in filmmaking, but it is also finding its way into more prosaic mediums, such as advertising and corporate communications.

Argentina-based design firm Icons8 offers “worry-free, diverse models on-demand using AI.” In essence they are offering digital humans on demand. The agency promises that their clients will “get the perfect model for your application by specifying age, ethnicity and physical attributes.” [12] Startup company Hour One licenses appearance and attributes of real-life people to generate synthetic characters available for purchase. Hour One boasts more than 40 clients, including real estate, e-commerce, digital health and entertainment firms. Among these clients is the international language school Berlitz, which uses these synthetic characters in teacher-led language courses.

According to the MIT Technology review, Berlitz wanted to increase the number of videos it offered, but struggled to do so using real human actors. They had to have production crews creating the same setup with the same actor over and over again, which proved to be “really unsustainable”. Berlitz now works with Hour One to generate hundreds of videos in minutes. [13] This approach, combined with the language localization demonstrated in the Beckham Malaria video, has the potential to revolutionize training for both staff and customers. In addition to language localization, materials can be tailored to specific cultural norms and necessities without the need for actors, sets and production crews.

As AI generation of voice and video becomes cheaper and more available, it is finding its way into more areas of the enterprise, especially for inward-facing applications. For example, synthetic media is beginning to challenge email and teleconferencing as a preferred communication channel. British startup Synthesia provides a platform that enables a user to read a script in front of a camera to generate a digital doppelganger. Forty minutes of reading provides enough information to replicate the reader’s speaking voice and cadences, along with their idiosyncratic facial expressions and muscle movements. Once the avatar is created, it can convert any text into a convincing rendition of the original person reading the text, even in a different language (see Figure 2).

Figure 2. The Synthesia Workspace



Due to performance reasons, we only reproduce audio during the preview.

Video script

Let's revisit the previous example: total investment of 100€; 20% (20€) into emerging markets and 80% (80€) into developed world. If you use DEGIRO, the minimum fee would account for 10% (!) of the total investment amount in the emerging markets ETF. If you use IB, the minimum fee would account for 20% (!) of the total investment amount in the emerging markets ETF. That is a lot to spend in fees.

Script language: English (change)

Request translation from English

Source: Synthesia.io

Financial firm EY has adopted Synthesia avatars in earnest, referring to them internally as "artificial reality identities" (ARIs). These digital doubles are used in emails, presentations and even client interactions. One EY partner uses his ARI to interact with Japanese clients in their native language. The EY team responsible for creating and managing the ARIs told Wired Magazine, "We're using it as a differentiator and reinforcement of who the person is. As opposed to sending an email … you can see me and hear my voice." Clients respond well to the ARIs. "It's like bringing a puppy on camera," EY told Wired. "They warm up to it." [14]

The advantages of synthetic avatars, or "digital humans," grow exponentially as their interaction capabilities approach real time. This is especially true when it would be helpful to give customers something to "warm up to." Consider a typical customer help desk or contact center. Interminable phone trees and sterile chatbots test both customer patience and loyalty. Replacing a faceless, text-based chatbot with a synthetic avatar that can visually express empathy and understanding could go a long way to de-escalate customer irritation while working toward a solution.

The underlying mechanism of the chatbot doesn't change significantly. The same decision tree and response selection would just be used to drive the digital human. Even when an interaction must be escalated to a human agent, the synthetic avatar could still preserve the anonymity of the agent while interacting with the customer. This would also hide the agent's often involuntary and derogatory facial expressions in response to unreasonable customer complaints and demands.

Both commercial and public service applications of synthetic media are still in their infancy. Even though the range of beneficial, legitimate uses is all but unlimited, today synthetic media is dwarfed by the number of illicit deepfakes. Both flavors of AI-generated content are, for better or worse, permanent elements of the online world and will grow in presence and prominence as the internet evolves. Even in their current nascent form, both synthetic media and deepfakes are our first glimpse of the metaverse.

Populating the Metaverse

The term "metaverse" was coined by speculative fiction author Neal Stephenson in his 1992 novel Snow Crash. Stephenson's metaverse described the successor to today's internet as an immersive, virtual environment in which humans use avatars to interact with each other and various software services and agents. More recently, the idea of the metaverse has been touted by Mark Zuckerberg as the future of Facebook and social media. He described the metaverse as "an embodied internet where, instead of just viewing content, you are in it." [15] Roblox mentioned the metaverse 16 times during its 2021 earnings call, and Unity Technologies did so eight times. [16] Even nation-states are staking their bets on an immersive, pervasive online future. In September 2021 the government of South Korea convened and funded the Metaverse Alliance, which includes more than 200 companies and institutions. [17]

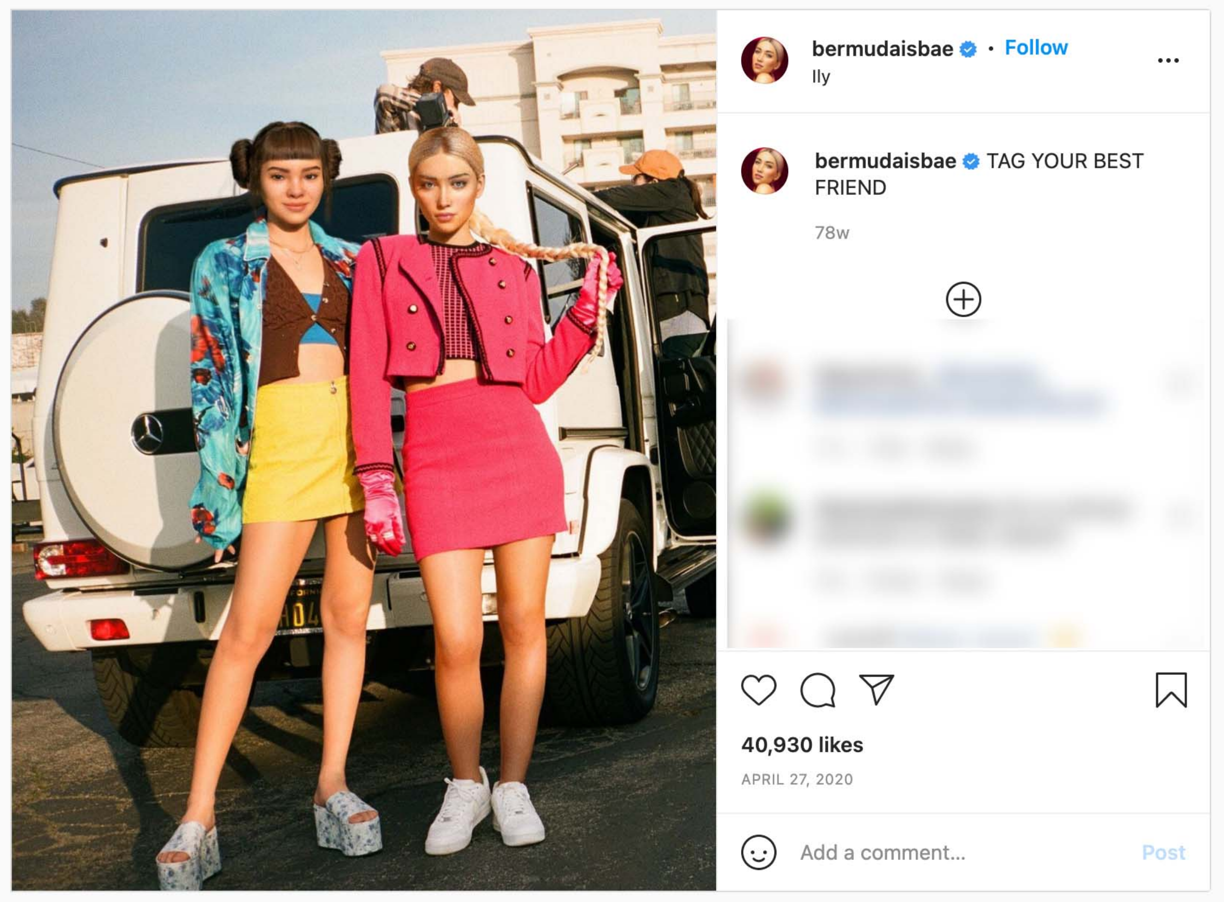
> **"He is not seeing real people, of course. This is all a part of the moving illustration drawn by his computer according to specifications coming down the fiber-optic cable. The people are pieces of software called avatars. They are the audiovisual bodies that people use to communicate with each other in the Metaverse."**
>
> *— N. Stephenson, Snow Crash*

At this point, the metaverse is largely a mix of aspiration and hype in equal measure. The Washington Post has even labeled it a "political strategy." [18] Gartner defines the metaverse as a collective virtual shared open space, created by the convergence of virtually enhanced physical and digital reality and physically persistent providing enhanced experiences.

The essential characteristics of the metaverse are that it is immersive, immediate and all-encompassing. Avatars, along with synthetic actors and environments, will be pivotal in enabling that ecosystem. Its first synthetic citizens are already taking up residence and consequently setting the tone for the neighborhood.

In 2018 an Instagram influencer named "Bermuda" hacked and took control of the account of "Lil Miquela," another influencer with over a million followers. Bermuda refused to return control of the account until "Lil Miquela" revealed her true nature to the world. Of course, both Bermuda and Lil Miquela were entirely synthetic avatars (see Figure 3). [20] Bermuda was eventually thwarted and retired. Time Magazine named Lil Miquela "one of the 25 Most Influential People on the Internet" and talent agency CAA signed her to an exclusive contract, where she is anticipated to earn $10 million for her creators in 2021. [21,22] Again, Lil Miquela only exists in software.

Figure 3. Synthetic Instagram Influencers Lil Miquela (left) and Bermuda (right)



bermudaisbae · Follow
lly

bermudaisbae TAG YOUR BEST FRIEND

78w

40,930 likes

APRIL 27, 2020

Source: Bermuda, Instagram.com

Feuding avatars, celebrity and otherwise, will be a common feature of a fully realized metaverse. So will avatars that are empowered to undertake more substantive tasks semiautonomously or otherwise,. AI-driven avatars executing blockchain smart contracts will be the metaverse equivalent of the signature machines now used to sign paychecks. Fully realized digital environments will replace the crude filters and backgrounds now used to hide home office clutter during Zoom meetings. In such an ecosystem, authentication, verification and trust will be paramount. Without these assurances, the next incarnation of the internet will be awash in deepfakes, leaving no place for legitimate synthetic media. The foundation for such a trustworthy environment needs to be established now, and to date we are on the wrong path.

Saving the Metaverse From the Liar's Dividend

Disinformation permeates the online world, so much so that "fake news" was declared the 2017 Word of the Year by Collins Dictionary. [23] This is resulting in the lowest levels of trust across institutions in decades. The 2021 Edelman Trust Barometer finds that across every type of institution — media, government, business and NGOs — trust has fallen to historic lows. In addition, people no longer trust their own ability to discern true information from false. As Edelman CEO Richard Edelman puts it, "This is the era of information bankruptcy." [24]

When people don't know what to believe, they simply choose to accept what they want to believe and dismiss any disconfirming information as false or fraudulent. This is a tremendous gift to bad actors. It is known as the "liar's dividend," in which any evidence showing something is untrue or faked is dismissed as being untrue or fake itself. A stunning example of this occurred shortly after George Floyd was murdered in May 2020. Within two weeks of the murder, despite the event being captured in real time by multiple witnesses, Winnie Hartstrong, a Republican congressional candidate, posted a 23-page "report" insisting that the murder never happened. Hartstrong claimed that the videos used as evidence of the murder were deepfakes, superimposing Floyd's face onto the body of an ex-NBA player in order to stir up racial tensions. [25]

> **"My biggest concern is not the abuse of deepfakes, but the implication of entering a world where any image, video, audio can be manipulated. In this world, if anything can be fake, then nothing has to be real, and anyone can conveniently dismiss inconvenient facts."**
>
> *— T. Sonnemaker. "'Liar's Dividend': The More We Learn About Deepfakes, the More Dangerous They Become." Business Insider, 13 April 2021.*

This example illustrates how deepfakes are near-perfect predators in the global information landscape. Not only do they enable bad actors to present and promote events that never occurred, they make it easier for bad actors to plausibly dismiss inconvenient events that actually did occur. While deepfakes are just the latest and most sophisticated manifestation of disinformation, this dual nature gives them more potential to do much more damage than any of their predecessors. Their existence and proliferation are especially effective at undermining trust in the digital economy. People have a much more visceral reaction to visual and audible information than to text. Not only does this make a more immediate and deeper impact on an individual, it enables the disinformation to spread faster and further. [26]

There is even evidence to suggest that deepfake media has the ability to implant false memories, the so-called Mandela effect. For example, in 2010, Slate presented a photo of then President Barack Obama shaking hands with former Iranian president Mahmoud Ahmadinejad. Slate then asked 1,000 of its readers whether they remembered seeing the photo. Twenty-one percent said they remembered seeing the photo when the event occurred. Another 25% said they remembered the event but couldn't recall specifically seeing the photo. One reader went so far as to editorialize on the handshake, saying: "I thought Obama was correct, snubbing Ahmadinejad so blatantly would have been a mistake." [27]

The handshake never occurred. The image was manufactured, as were the memories of the Slate readers. None of them had seen the image before being asked if they remembered the event. This experiment illustrates the shortcomings of current approaches to combating disinformation in general, and deepfakes in particular. To date, efforts to counter disinformation in all forms have focused on detecting and discrediting. When a deepfake draws enough attention, it may be scrutinized, discovered to be faked and labeled as such. By that point it is far too late. The damage is done. People have already internalized the imagery, and even if they can consciously and rationally acknowledge that it is fake, the impression has been made and will remain. When deepfakes enter the metaverse and become fully immersive sensory experiences, such post hoc remediation efforts will be even more futile.

> "Falsehood flies, and truth comes limping after it, so that when men come to be undeceived, it is too late; the jest is over, and the tale hath had its effect."
>
> *— Jonathan Swift*

The pervasiveness and perniciousness of deepfakes is already driving public figures to extreme measures. Some are creating digital alibis with lifelogging, recording every moment of their lives with time stamped and geocoded video in order to prove they were not at a place and time or engaged in an activity a deepfake purports to have captured. [28] Some have taken a simpler approach by getting secret tattoos in places "not normally visible" in order to prove that the body on display in a deepfake video is not theirs. [29]

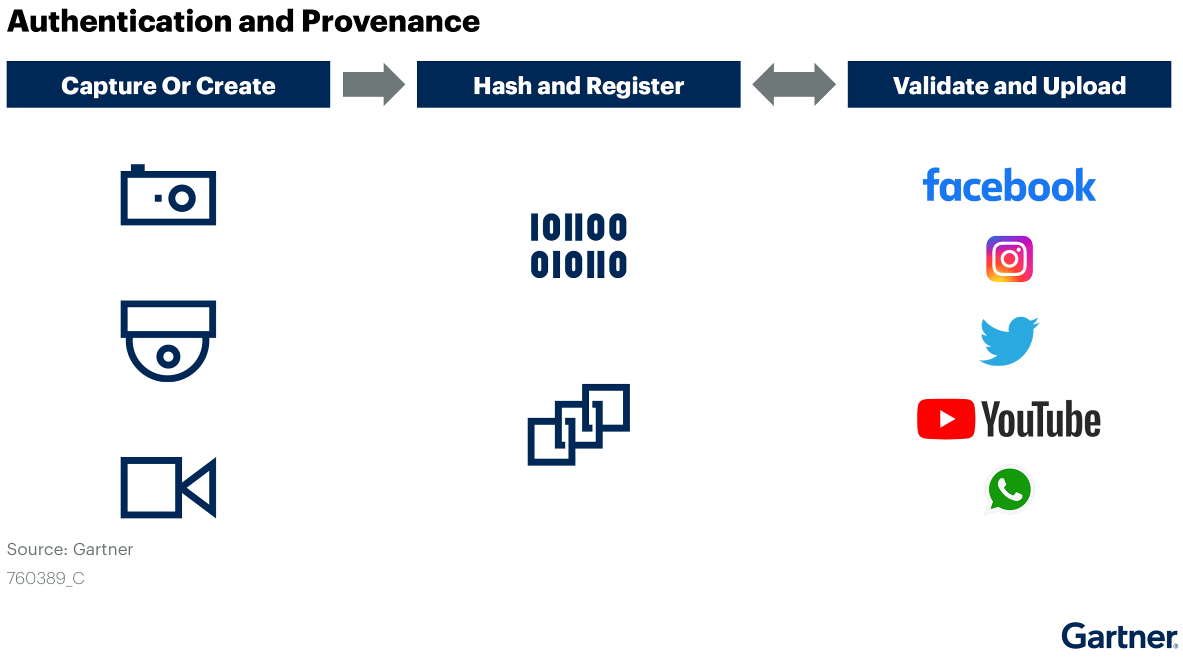
Detection is an important tool in combating deepfake disinformation, and it will remain so. But detection methods must evolve to match the advancing sophistication of deepfakes. Efforts are underway in this area, but even the most advanced detection mechanisms will always be reactive and ultimately insufficient. The ecosystem itself, both the internet of today and the metaverse of tomorrow, must be trustworthy. This requires robust provenance mechanisms, ensuring authenticity and legitimacy throughout the information life cycle. Together, detection and provenance can ensure an online environment in which illicit deepfakes have little sway and synthetic media can flourish.

Protection Beyond Detection

In our daily lives, we regularly depend on knowing where something came from, and that it hasn't been tampered with. Bottles of aspirin and tubes of toothpaste, boxes of cereal and bags of potato chips all come with tamper-evident seals. If the seal is broken, we know immediately that something isn't right with the product and that we shouldn't consume it. If the issue is significant, we can examine the supply chain for the product to pinpoint where the tampering occurred. Synthetic media can provide the same assurances using blockchain.

Blockchain provides an immutable record of transactions. More formally, blockchain is an expanding list of cryptographically signed, irrevocable transactional records shared by all participants in a network. Each record contains a time stamp and reference links to previous transactions. These characteristics make blockchain an ideal framework for comprehensive synthetic media authentication and provenance (see Figure 4).

Figure 4. Authentication and Provenance



Source: Gartner

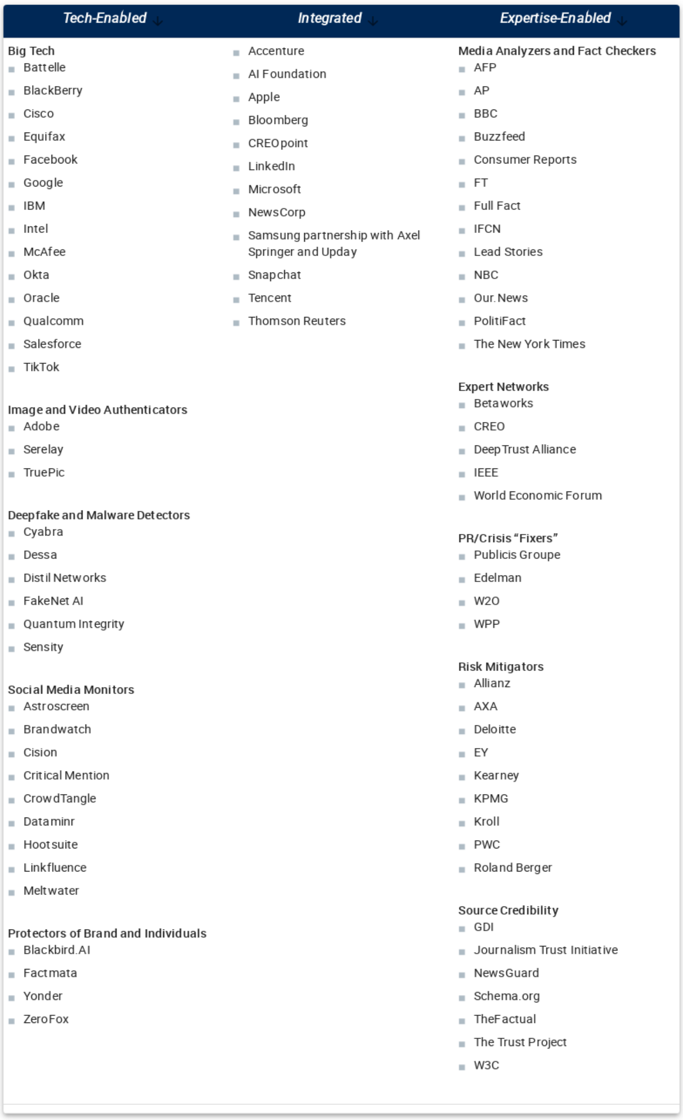
760389_C

Although scattered and isolated, all of the elements necessary to create such an end-to-end authentication and provenance architecture already exist in the marketplace (see Table 1). For example, companies like Factom and Truepic provide publishing platforms that generate hashes of media and organize that data for blockchain provenance. What is lacking is a cohesive and coordinated effort to weave them together into a ubiquitous and comprehensive solution.

Efforts to change this are already underway by organizations such as the DeepTrust Alliance and the News Provenance Project. Lawmakers are recognizing the need and are attempting to take action, such as the “Deepfake Reporting Act,” introduced in the U.S. Senate in October 2019, and California’s AB730 and AB602, which address deepfakes in politics and pornography. [30] What is missing is incentive for the platforms that depend on deepfake-driven engagement for their revenue streams.

Table 1: The Synthetic Media Landscape

(Enlarged table in Appendix)



Tech-Enabled	Integrated	Expertise-Enabled
Big Tech Battelle BlackBerry Cisco Equifax Facebook Google IBM Intel McAfee Okta Oracle Qualcomm Salesforce TikTok **Image and Video Authenticators** Adobe Serelay TruePic **Deepfake and Malware Detectors** Cyabra Dessa Distil Networks FakeNet AI Quantum Integrity Sensity **Social Media Monitors** Astroscreen Brandwatch Cision Critical Mention CrowdTangle Dataminr Hootsuite Linkfluence Meltwater **Protectors of Brand and Individuals** Blackbird.AI Factmata Yonder ZeroFox	Accenture AI Foundation Apple Bloomberg CREOpoint LinkedIn Microsoft NewsCorp Samsung partnership with Axel Springer and Upday Snapchat Tencent Thomson Reuters	**Media Analyzers and Fact Checkers** AFP AP BBC Buzzfeed Consumer Reports FT Full Fact IFCN Lead Stories NBC Our.News PolitiFact The New York Times **Expert Networks** Betaworks CREO DeepTrust Alliance IEEE World Economic Forum **PR/Crisis "Fixers"** Publicis Groupe Edelman W2O WPP **Risk Mitigators** Allianz AXA Deloitte EY Kearney KPMG Kroll PWC Roland Berger **Source Credibility** GDI Journalism Trust Initiative NewsGuard Schema.org TheFactual The Trust Project W3C

Source: Adapted from DeepTrustAlliance.org

Inflammatory and salacious content drive engagement far more effectively than accurate and even-handed communication. [31] This is why social and media platforms boost and recommend such content. Veracity and authenticity are secondary considerations, if they are considered at all. As Facebook is discovering, that business model may ultimately prove to be their undoing. [32]

Deepfake disinformation is not just a problem for some future, as yet unrealized metaverse. A survey of 25,000 internet users conducted by Ipsos on behalf of the Centre for International Governance Innovation (CIGI) found that “distrust in the internet is causing global citizens to disclose less information online, use the internet more selectively, and make fewer online purchases among other precautions.” [33] This continues a consistent trend in loss of online trust over the five years the study was conducted. The report concludes that this loss of trust is, and will continue to be, a major impediment to the global digital economy. There is no reason to expect it to improve without fundamental changes to how information is shared, authenticated and verified.

Evidence

[1] Deepfake Porn Is Ruining Women’s Lives. Now the Law May Finally Ban It, MIT Technology Review.

[2] Campaigns Must Prepare for Deepfakes: This Is What Their Plan Should Look Like, Carnegie Endowment for International Peace.

[3] David Beckham Launches the World’s First Voice Petition to End Malaria, Malaria Must Die.

[4] Connecting in the Metaverse: The Making of the GTC Keynote, NVIDIA (via YouTube).

[5] N. Stephenson, “Snow Crash,” Bantam Books, 1993.

[6] Photo Tampering Throughout History, Georgia Tech College of Computing.

[7] We Are Truly F***ed: Everyone Is Making AI-Generated Fake Porn Now, Vice.

[8] Deepfake Voice Tech Used for Good in David Beckham Malaria Campaign, PRWeek.

[9] The Pros and Cons of Dubbing and Subtitling, European Journal of Communication 17(13).

[10] Many Are Upset That Anthony Bourdain Documentary Roadrunner Used an AI Deepfake of His Voice, The Mary Sue.

[11] Then and Wow: Deepfake Technology Introduces a New Wave of Storytelling in the Sports World, SportTechie.

[12] Generated Photos Team Releases API for Face Images Made by AI, Icons8 Blog.

[13] People Are Hiring Out Their Faces to Become Deepfake-Style Marketing Clones, MIT Technology Review.

[14] Deepfakes Are Now Making Business Pitches, Wired.

[15] Mark in the Metaverse, The Verge.

[16] The Metaverse Takes Shape as Several Themes Converge, Yahoo Finance.

[17] South Korea’s ‘Gen MZ’ Leads Rush Into the ‘Metaverse’, Reuters.

[18] How Facebook’s ‘Metaverse’ Became a Political Strategy in Washington, Washington Post.

[19] The Metaverse Primer, MatthewBall.vc.

[20] CGI ‘Influencers’ Like Lil Miquela Are About to Flood Your Feeds, Wired.

[21] The 25 Most Influential People on the Internet, Time.

[22] Miquela, the Uncanny CGI Virtual Influencer, Signs With CAA, Variety.

[23] ‘ Fake News’ Named Word of the Year, Yahoo Life.

[24] 2021 Edelman Trust Barometer Reveals a Rampant Infodemic Is Fueling Widespread Mistrust of Societal Leaders, Edelman.

[25] Republican Candidate Shares Conspiracy Theory That George Floyd Murder Was Faked, The Independent.

[26] The Spread of True and False News Online, Science.

[27] We’re Underestimating the Mind-Warping Potential of Fake Video, Vox.

[28] Deepfakes and the New Disinformation War, Foreign Affairs.

[29] Defending Against Deep Fakes with Lifelogs, Watermarks … and Tatts?, The CyberLaw Podcast.

[30] Two New California Laws Tackle Deepfake Videos in Politics and Porn, Davis Wright Tremaine LLP.

[31] Designing Outrage, Programming Discord: A Critical Interface Analysis of Facebook as a Campaign Technology, Technical Communication.

[32] Facebook Is Weaker Than We Knew, The New York Times.

[33] CIGI-Ipsos 2019 Global Survey on Internet Security and Trust, Center for International Governance Innovation.

Note 1 Roots of the Word “Maverick”

Derived from the name of Texas rancher Samuel Maverick and his steadfast refusal to brand his cattle, "maverick" connotes someone who willfully takes an independent — and frequently disruptive or unorthodox — stand against prevailing modes of thought and action.

Recommended by the Author

Some documents may not be available as part of your current Gartner subscription.

Maverick* Research: How Disinformation Is Destroying Business and How to Fight Back

Maverick* Research: Welcome to the Splinternet — How Internet Fragmentation Disrupts Business and Threatens Society

Maverick* Research: Digital Humans Will Drive Digital Transformation

Top Strategic Technology Trends for 2022: Generative AI

Innovation Insight for Generative AI

Table 1: The Synthetic Media Landscape

Tech-Enabled ↓	*Integrated* ↓	*Expertise-Enabled* ↓
Big Tech ▪ Battelle ▪ BlackBerry ▪ Cisco ▪ Equifax ▪ Facebook ▪ Google ▪ IBM ▪ Intel ▪ McAfee ▪ Okta ▪ Oracle ▪ Qualcomm ▪ Salesforce ▪ TikTok **Image and Video Authenticators**	▪ Accenture ▪ AI Foundation ▪ Apple ▪ Bloomberg ▪ CREOpoint ▪ LinkedIn ▪ Microsoft ▪ NewsCorp ▪ Samsung partnership with Axel Springer and Upday ▪ Snapchat ▪ Tencent ▪ Thomson Reuters	**Media Analyzers and Fact Checkers** ▪ AFP ▪ AP ▪ BBC ▪ Buzzfeed ▪ Consumer Reports ▪ FT ▪ Full Fact ▪ IFCN ▪ Lead Stories ▪ NBC ▪ Our.News ▪ PolitiFact ▪ The New York Times **Expert Networks** ▪ Betaworks

Tech-Enabled ↓ *Integrated* ↓ *Expertise-Enabled* ↓

- Adobe
- Serelay
- TruePic

Deepfake and Malware Detectors

- Cyabra
- Dessa
- Distil Networks
- FakeNet AI
- Quantum Integrity
- Sensity

Social Media Monitors

- Astroscreen
- Brandwatch
- Cision
- Critical Mention
- CrowdTangle
- Dataminr
- Hootsuite
- Linkfluence

- CREO
- DeepTrust Alliance
- IEEE
- World Economic Forum

PR/Crisis “Fixers”

- Publicis Groupe
- Edelman
- W2O
- WPP

Risk Mitigators

- Allianz
- AXA
- Deloitte
- EY
- Kearney
- KPMG
- Kroll

Tech-Enabled ↓	Integrated ↓	Expertise-Enabled ↓
- Meltwater		- PWC - Roland Berger
Protectors of Brand and Individuals - Blackbird.AI - Factmata - Yonder - ZeroFox		**Source Credibility** - GDI - Journalism Trust Initiative - NewsGuard - Schema.org - TheFactual - The Trust Project - W3C

Source: Adapted from DeepTrustAlliance.org