Received: 1 August 2023 | Revised: 28 September 2023 | Accepted: 29 September 2023

DOI: 10.1002/wfs2.1505

PERSPECTIVE

WIREs FORENSIC SCIENCE WILEY

The metaverse—Not a new frontier for crime

Angus McKenzie Marshall[1] | **Brian Charles Tompsett**[2]

[1]Department of Computer Science, University of York, York, UK

[2]Department of Computer Science, University of Hull, Hull, UK

Correspondence
Angus McKenzie Marshall, Department of Computer Science, University of York, York, UK.
Email: angus.marshall@york.ac.uk

Edited by: Kim-Kwang Raymond Choo, Editor

Abstract

Law enforcement co-ordination agencies have recently issued position/guidance documents relating to the potential for VR environments (the "Metaverse") to become new environment for criminal activity, and calling for additional work to enhance investigative capability. By reviewing the historic development of VR and comparing it with the appearance of the WWW, the authors propose that the situation is not as dire as the issued documents may suggest, but represents an evolutionary rather than revolutionary step in online experiences. They conclude, therefore, that while ability to examine VR presentation/interaction devices may be useful, continued development of ability to examine online systems remains essential.

This article is categorized under:

Digital and Multimedia Science > Multimedia Forensics
Digital and Multimedia Science > Cybercrime Investigation
Digital and Multimedia Science > Artificial Intelligence

KEYWORDS

crime, digital evidence, investigation, metaverse, virtual realtiy

1 | INTRODUCTION

1.1 | Defining the metaverse

Interpol's "Technology Assessment Report on Metaverse" (Interpol, 2023) states "The Metaverse is considered to be the next stage in the development of the Internet." Powered by a broad range of technologies, including virtual reality (VR), augmented reality (AR), and edge computing, it aims to enable people around the world to access shared 3D virtual environments. Using an internet connection and specialized hardware like VR headsets or haptic suits (allowing the virtual environment to provide touch and force feedback to the user via vibration or restriction of movement), individuals can enter these virtual spaces via avatars, creating a sense of "virtual presence." Europol (2023)) have a similar, but less technology-oriented description, which includes the concept of a "digital twin" as a visually similar representation of the user in the simulated space.

This definition tends to align with the outcome of Ritterbusch and Teichmann's review of metaverse literature (Ritterbusch & Teichmann, 2023). Whilst noting a lack of consensus on the use of the term, they estimated that common definitions of the metaverse currently center around the idea of a "three-dimensional online environment in which users represented by avatars interact with each other in virtual spaces decoupled from the real physical world"

TABLE 1 Modes of experience.

	Interactive—user has freedom to take any action at any time	**Partial interactive—user chooses actions from a set specific to circumstances, dictated by another party**	**Passive—user can take no action but experience is controlled by another party**
Immersive—MV supplants MS as primary experience (not quite there yet)	Open World VR	Business applications—presenting and simulating, games with goals/stories	Business applications—modeling, simulation presentation to client
Partial immersive—MS can intrude on experience but MV dominates most senses	Open World VR	Business applications—presenting and simulating, games with goals/stories	Business applications—modeling, simulation presentation to client
Windowed—MV is experienced through only one or two senses and presented in a limited way	SecondLife, OpenSim, Open World games	First person games, AR on mobile devices	Movies, TV—recorded entertainment
Projective—MV projects into MS	AR with AI assistant	AR with programmed assistant	Projected content (HUDs in vehicles, etc.)

Abbreviations: AR, augmented reality; MS, meatspace; MV, metaverse.

(Ritterbusch & Teichmann, 2023). In other words, a fundamental feature of the metaverse is the presence of a 3D immersive interface.

Perhaps the most striking element of these common descriptions of the metaverse is how many of the technologies solely relate to "projection" of the user into a virtual environment through the use of VR headsets, detailed 3D worlds, and haptic controls. Little consideration is given to the potential for the metaverse to be projected into "meatspace,"[1] nor how current technology allows a different, less-immersive, type of projection to be enabled through windows into the virtual world in the form of general-purpose browsers and task-specific applications such as games. Table 1 summarizes our view of the modes of metaverse experience available, based on the authors' personal experience.

In this document, we suggest that this immersive interactive interface-centerd approach to defining the metaverse may create serious challenges for stakeholders in the public protection domain. We offer an alternative approach to defining the metaverse, for the purposes of public protection, which is presentationally agnostic and instead centerd around key interactions that stakeholders posit will occur in future metaversal environments. In doing this, we propose that the following four statements may be axiomatic:

1. the transition into a "full" metaverse will be gradual rather than abrupt;
2. that such a transition is already underway, and has been for decades;
3. that serious metaverse-related risks to public protection are already widespread; and
4. that a focus on future presentation technology may hamper public protection stakeholders in identifying such threats.

2 | BACKGROUND

In many ways, the immersive interactive interfaces are not conceptually novel, and have their roots in the history of computing, with work done by Engelbart and Lehtman (1988; Information Systems, Networking, Personal Computers, User Interfaces, The Mouse), Sutherland (1968; First head-mounted stereoscopic display for VR/AR), Krueger (1977; computer-generated immersive and responsive environments), and others who contributed to the development of simulated environments, interaction methods, and refinement of presentation and interaction technologies (Bown et al., 2017; Vertucci et al., 2023). Contemporary implementations build on the principles established in this earlier work, improving its capabilities, lowering its price, and packaging in a more attractive and user-acceptable way, thus addressing some of the factors identified by Hess and Mutterlein (2017). In particular, the issues related to low image resolution (general dissatisfaction about the overt artificiality of the virtual environment) and lag (delay between user input and the environment responding or updating to reflect this) have been reduced through normal evolution of

technology. (Other issues, such as continued awareness of the real world and concerns about what is happening in it during immersion in the virtual, or something akin to motion sickness whilst in the simulated environment, or adjusting to the return to real world may require additional work to solve as they are related to physiological effects.) The net effect of this is that what was once a cumbersome and fragile presentation mechanism has become less-so, making it more comfortable to wear, more portable and potentially more attractive to the end user. This technology, however, mainly addresses the way a virtual environment is presented to a user with normal stereoscopic vision, and the way a user with normal ranges of limb motion can interact through the use of hand-held or motion capture controllers, potentially causing accessibility issues for others (Mott et al., 2020).

However, it is unclear whether these presentational technologies are necessary for the existence of the kinds of metaversal experiences and interactions, which are relevant in the public protection and criminal investigation domain. In parallel with these advancements in presentation, and leading it by several years, there has been a huge growth in the development of virtual environments, culminating in current "immersive" multi-player online games or interactive fiction with near-cinematic graphics and sound effects. Social media, too, has grown as an alternative facilitator for human interaction, as have online collaboration platforms, such as Zoom, Microsoft Teams, and so forth, with their uptake accelerated by changes in working styles engendered by public health measures and a recognition that, for many purposes, physical presence in a place of work may not be necessary or desirable.

It should be borne in mind, however, that some of these technologies are problematic in themselves, with video-conferencing being a prime example, because of the way in which human interaction is mediated and presented in an unnatural way. This can lead to fatigue, dissatisfaction, or resistance to use. Ballenson (2021) suggests that there may be four causes for this in the context of video-conferencing: "Excessive amounts of close-up eye gaze, cognitive load, increased self-evaluation from staring at video of oneself, and constraints on physical mobility" (Box 1). Of these, it is likely that at least two (constraints on physical mobility and cognitive load) will extend into immersive 3D worlds. The issue of self-evaluation may also arise from the use of an avatar of which the user is aware, but dissatisfied with for some reason (e.g., lack of ability to present themselves as they wish to), while the issue of excessive close-up eye gaze may even be exacerbated by the use of 3D headsets.

2.1 | Investigatory views of the metaverse

There are, in effect, two competing definitions of the metaverse, with different implications for investigation and "policing."[2]

In the Interpol/Europol view, the existence of metaverse technology represents a radically new way to interact with machines and humans. The technology thus creates an inflection point, engendering radical change in use and experience of online services and new opportunities for crime, including crimes that may never have existed before. This definition concentrates, we suggest, on the presentational/experiential aspects of the technology almost to the exclusion of consideration of the foundations on which it is built. It also tends to suggest that new forms of interaction are created by the technology, rather than existing modes of interaction being mediated and presented differently by the technology. This seems to give rise to a hypothesis that the existence of new technology is itself, sufficient to create the conditions for some new form of crime, contrary to the assertion that there are no new crimes, merely "old wine in new bottles" (Marshall & Clarkson, 2008).

BOX 1 Zoom fatigue—an alternate view

These authors would argue, from personal experience, that the absence of eye gaze is a potentially bigger problem, having spent significant amounts of time starting at screens full of black boxes with just names on them, instead of seeing human faces, whilst trying to conduct tutorials during lockdown. This leads to an increase in cognitive load due to the absence of non-verbal feedback cues from participants. This situation is likely to be exacerbated by the presence of human-like avatars, which may exhibit no, very few, or delayed visual cues during interactions.

For example, for centuries, human beings relied on being proximate to one another in order to have an audible conversation. The creation of the telephone, and then the use of audio and video over Internet channels changed the means of transmission, but not the content or intent of the communication itself. It may have become easier to commit certain types of crime at a distance, with improved potential anonymity (e.g. "boiler room" stock fraud) over the telephone, but the telephone itself did not create a new type of crime, just a new way to commit an old crime.

In the other definition, we view the immersive vision of the metaverse as largely an expansion of the set of modes of presentation and interaction, creating additional opportunities for common meatspace sensory experiences to be perceived, but in a more distributed or remote form (i.e., those sharing the experience do not need to be in the same location). This was summarized in Marshall and Clarkson (2008) as "The crimes committed are not novel—though the modalities may be. Prior study has concluded that technology may facilitate or even broaden the scope of a given criminal act, but the use of technology is an extension rather than creation of a criminal class."

Given that crime can be defined as "that which is prohibited by law," we suggest the latter view is more realistic until, and unless, public opinion leads to the creation of new laws that explicitly prohibit particular types of online activity. It is worth noting, at this stage, that any such laws will need to be very carefully crafted in order not to be either circumvented by changes in modus operandi, or superseded by changes in technology (Marshall, 2015).

Recent events, such as the Cambridge Analytica case and allegations of election interference have shown that new online services do not cause new types of abusive behavior or crime but simply facilitate them in a way that is similar to that previously seen in older media, prior to regulation intended to address these abuses, but on a much larger scale. Criminal or abusive use of technology is not, however, a new phenomenon. In the case of the Internet, the Morris Worm of 1988 (Furnell & Spafford, 2019) and Clifford Stoll's experience of tracing a hacker (Stoll, 1989) represent two of the most well-known early instances of computer misuse, but there can be little doubt that any technology, which increases access to information, makes communication between people easier, or which manipulates something of value to human beings, will be examined by those with malicious intent, and, if at all possible, subverted for their own ends. Further examples of this include criminal use of Whatsapp (Marshall, 2018) and other communications software, adoption of mobile phone call charge management techniques to obfuscate relationships between callers and callees (Marshall & Miller, 2019), the continuing creative misuse of social media to target potential victims (Salter, 2017), adoption and use of the Dark Web (Saleem et al., 2022), and so on. The reality is that, since access to the Internet became available to the public, it became attractive to criminals because of the large pool of potential victims it offered, coupled with the potential for miscreants to hide their own identities (with varying degrees of success). It is commonplace for criminal trials, ranging from counterfeiting of goods through drugs distribution, sexual abuse and murder, to contain some element of digital evidence, usually showing either contact between relevant parties, or accessing of information relevant to the charges made.

Underpinning all of these online services, from social media and collaborative working, through multi-player games to immersive collaborative environments is common Internet technology in the form of standard IP networking and agreed protocols, usually enabling interaction with some form of centralized control and/or storage system with the edge-computing element primarily acting as a presentational and human-interface client. Even in a decentralized system, modeled perhaps on Web 3.0 (Liu et al., 2022), there will still be a need for some form of co-ordination and communication between different elements, potentially relying on data being propagated between nodes as required, rather than stored centrally—something of a throwback to the early days of email and NNTP (Kantor & Lapsley, 1986) and currently embodied in the growing concept of the fediverse (Cohn & Mir, 2022) or federated universe.

2.2 | A metaverse communication model

The standard IP layered model (Figure 1) concerns itself solely with application to application communications at the upper level, that is, communication between software elements. This model does not include any consideration of how those software elements are being used, nor of the experiences they provide to the users. However, a layered model is useful as it shows how upper layers can be supported by different technologies in the lower layers, and how each layer exists largely independently of the layer below it. Thus, at the highest level, no detail of how data are actually represented by any of the lower layers is known or required.

For discussion of the metaverse, and criminal opportunities within it, we need to consider interaction with humans, engendering a requirement for consideration of metaverse entity-to-entity communication. This recognizes the fact that some interactions will be between human and application alone while human to human communications are mediated or facilitated by some form of application (i.e., human to human is, at a minimum, human to application to human).

Application (Program to Program)	HTTP	TLS/SSL	SMTP	POP-3	SNMP	DNS	XMPP	etc.
Transport (Management of packetized data)	TCP / UDP							
Network (station to station)	IP / ICMP / ARP							
Physical (connections and signalling – wired or wireless)	Data Link							
	Physical							

FIGURE 1 IP network layered model.

Interaction		Human : Human	Human : Non-Human	Non-human : non-human
Enabler / Mediator		Client - user presentation and interface (Browser, email client, chat client, mobile app., telnet, ssh, ftp, nntp, VR headset, AR headset, etc.)	(not required for non-humans)	
IP Network layers	Application	HTTP, TLS/SSL, SMTP, POP-3, SNMP, DNS, XMPP, etc.		
	Transport	TCP / UDP		
	Network	IP / ICMP / ARP		
		Data Link		
	Physical	Physical		

FIGURE 2 Metaverse communication layered model.

Conventionally, in investigations, evidential artifacts are recovered from applications and their data storage. These artifacts represent something about how those applications were communicating or communicated with via the IP network represented by Figure 1 and typically only at one end of the transaction, in the form of cached, logged, or recorded data. For simple applications, this may be adequate as communication is carried out over a limited number of protocols. In more complex investigations, however, it may be more appropriate to attempt to use live network forensics, where data from the lower layers are captured. This allows all activity on that part of the network to be analyzed in order to understand not only the activity arising from a single application, but all activity present, from all active applications, during the period of interest.

In considering the metaverse, an enhanced communication model (Figure 2) may be useful in order to assist in the identification of evidential opportunities based on user experiences and behaviors, bearing in mind that any VR system will use multiple application layer protocols to generate something that the human participants experiences as a coherent immersive environment. The purpose of the proposed model is, therefore, to act as a reminder that when a human being reports a particular event, the investigator will need to consider the various sensory modalities involved in that event and hence the underlying software and protocols used to generate it.

This model allows a more considered view of the metaverse to be taken. Rather than viewing it as a "game changer" as Interpol describe it, we see it as an evolutionary step, providing new ways to present services that most likely already exist in one form or another. The fundamental opportunity that the metaverse technologies present to the user is additional aggregation of services under a common interface, rather than the creation of new services that have no existing

parallels. The metaverse client can, therefore, be compared to the web browser of 1990 (Berners-Lee, 1989) or the competing, text-only, Gopher client of 1991 (McCahill & Anklesaria, 1994) insofar as it could allow a disparate group of competing and complementary services to be presented via a common interface metaphor.

At the time of writing, uptake of VR technology has been quite low, akin to the uptake of web and gopher clients, and similar software such as ftp (file transfer protocol, for data transfer), telnet (remote terminal sessions for interaction), and so forth in the earlier part of the 1990s. Prior to 1995 use of such software was largely confined to academics and enthusiasts or hobbyists, not least because of the relative difficulty in obtaining the software in the first place. Networking required additional hardware and software, which were perceived as expensive and difficult to install and configure for less-knowledgeable users.

In fact, we would argue that the "game changer" around World-Wide-Web was not so much the existence of the web itself, but the inclusion of a web browser and simple dial-up networking interface in Microsoft's Windows 95, which made the Internet and Web more readily accessible to home users. As the dominant platform in domestic settings (possibly because of the inclusion of simple to use networking and web browsing), this allowed non-expert users to experience the web for the first time, without significant additional cost or effort, and encouraged hardware vendors to further enable this by including modems in their offerings in order to make best use of the new features bundled with the operating system. This may be, to some extent, likely to have been a side-effect of the initial primary motivation, promoted by internet service providers, for personal Internet connections as a means to access to email.

This viewpoint may be considered contentious, given that speed with which the Internet and World Wide Web were developing in the 1990s, but historical and contemporary reports tend to give credence to the idea that Windows 95 was, if not the primary driver, at least a major element in the increase in usage of Internet and Web services during that period.

- "The real boom started in 1995, thanks to Netscape going public on August 9 and the launch of Microsoft Windows 95 on August 24." Netscape's IPO (initial public offering) was followed avidly by the news media, and it was a spectacular success: the share price started at $28 and climbed to $75 before closing at $58. A small, unprofitable company had made lots of people rich, mainly because of excitement about the potential of the web.
- "Shortly afterwards, Windows 95 got the biggest launch in software history. This helped kickstart sales of affordable PCs that could surf the web. Netscape was featured at the launch, but Microsoft had developed its own browser, Internet Explorer, using code licensed from Mosaic. This marked the start of the acrimonious Browser Wars" (Schofield, 2016).
- "Windows 95 also made getting online very easy. I played around with getting internet access working on my Windows 3.11 computer, and it wasn't an easy process—it certainly wasn't something most people would want to do. Windows 95, on the other hand, didn't need you to get a winsock.dll working to surf the net. This was the start of a real revolution, and by virtue of the massive number of Windows users, must have played a big part in boosting the adoption of online services." (Morris, 2015).
- "...after Windows 95 arrived, tech quickly became a standard part of people's lives. The Internet became mainstream, homes got connected, and software became something everyone uses." (Dash, 2020).
- "Because critical mass for interactive technologies is 'all-or-none', (Markus, 1987), the Web will not be successful as a commercial medium until it achieves critical mass. An important first step in any marketing program is therefore the determination of how many people are on the Internet and what they are doing there (Hoffman & Novak, 1994). It is also necessary to define and estimate segments of Web behavior based on customer need. The economics of the Web can then be examined for each specific case to determine if the return on investment meets financial targets" (Hoffman et al., 1995).
- "...to understand the impact of Windows 95, we have to go back to an astute observation by one of the key elders of computing and networking. Bob Metcalfe, the inventor of Ethernet, once observed that a network's effect is proportional to the square of the number of connected users of the system (n^2). That law is called the Metcalfe's Law. The launch of Windows 95 acted as a steroid for Metcalfe's law. The more people got on the network using Windows 95-based computers, the more useful the network became. The more useful the network was, the more people wanted to be on it. The web would become the first and ultimate app. It would also set a stage for what would become a society defined by the symbiotic relationship between the computing devices and the networks that connected them." (Malik, 2020).

Hobbes' Internet Timeline (Zakon, 2018; Figure 3) confirms that the boom accelerated in late 1995, with a marked increase in the rate of domain registrations, a coarse indicator of increased interest in the Internet. This is shortly after the IPO of Netscape and the release of Windows 95, both of which were high-profile events in popular media.

Similarly, Hobbes' data on web hosts also shows a marked increase in number of sites, and the rate of their creation, again, starting shortly after the release of Windows 95 (Figures 4 and 5).

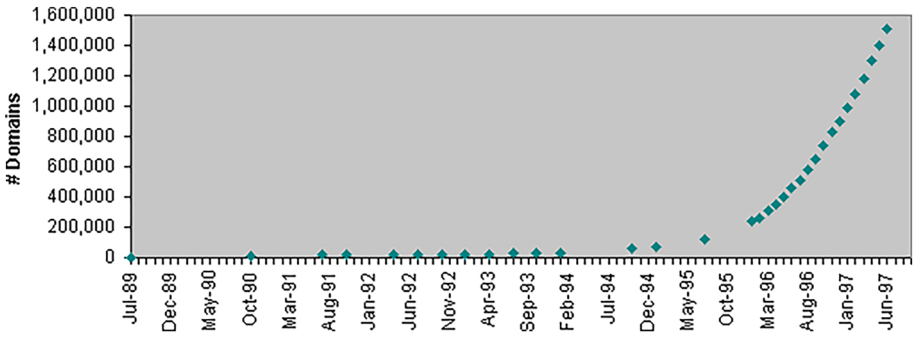

FIGURE 3 Hobbes' Internet Timeline 1989–1997 Domain Registrations. Rapid growth appears after the release of Windows 95, suggesting a growth in demand for permanent online presences (reproduced by permission).

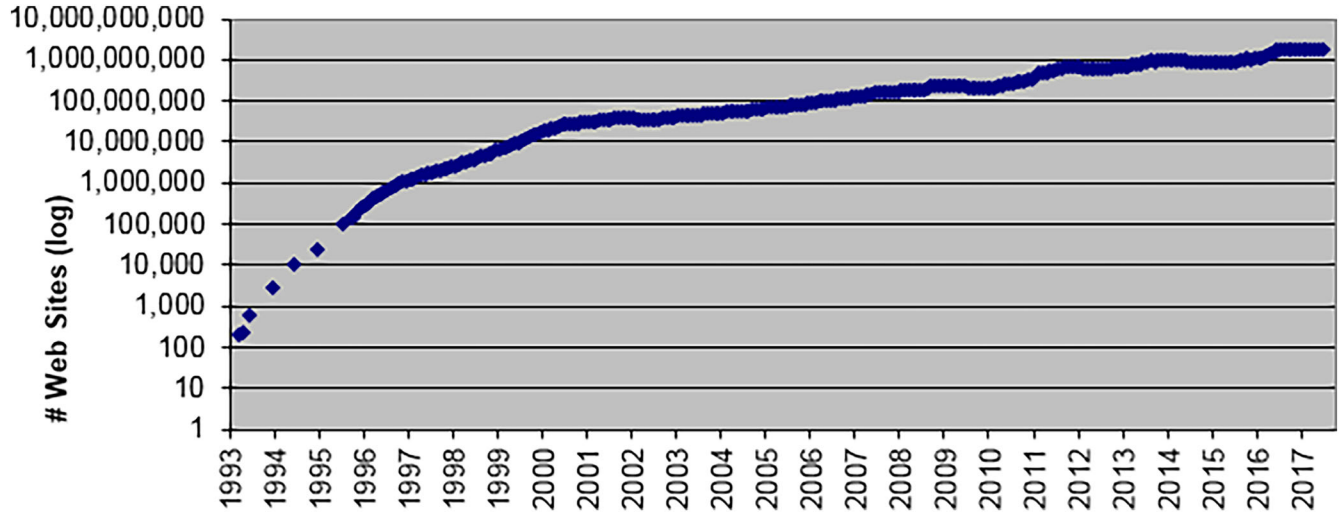

FIGURE 4 Hobbes' Internet Timeline graph of total web hosts (log scale). Again, this suggests a rapid growth in demand for online presence post-1995 (reproduced by permission).

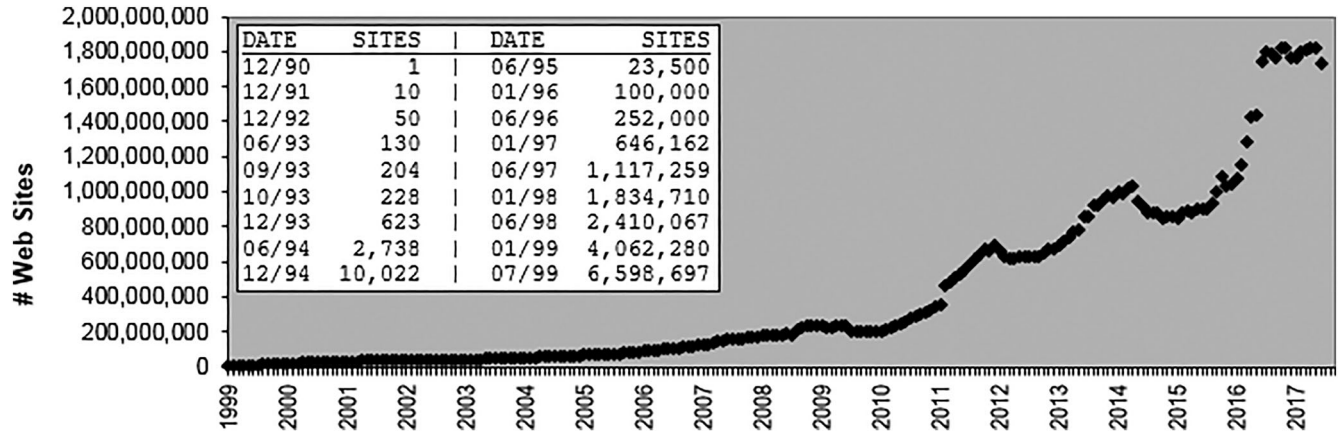

FIGURE 5 Hobbes' internet timeline graph of known web sites over time. Note the rapid increase between June 1995 and June 1997 shown in the numerical data (top left) (reproduced by permission).

This suggests that the necessary critical mass for widespread adoption was being reached.

We posit that ready availability of a web browser (Internet Explorer, even if only used to download another browser) on a simple to use platform with networking readily available led to a recognition that the web had become a more mature and significant platform, incentivizing the creation of more new domains and sites, thus encouraging more consumers to connect to it, and so on. Interestingly, even though web browsers included the ability to communicate over other protocols, including gopher and ftp, it seems that the relative ease of use of HTML, flexibility of HTTP's ability to deliver any type of content without requiring extensions to the protocol, and the provision of free web hosting, or hosting bundled with dial-up service provision, led to HTTP becoming a dominant protocol and other services becoming somewhat moribund.

Moreover, because the web browser is just another application on the desktop, it can be dipped into as required, for work or entertainment, and was not designed or intended to replace any existing technologies, but rather to co-exist and complement them. Its evolutionary path has led to a state where it is capable of replacing many features of a general purpose computer, embodying many of the features of a virtualized operating system within modern browsers, but it has been a slow process rather than a step-change. The addition of server and client side processing, coupled to web software and the lightweight flexible HTTP, created a situation where distributed computing became cheap and, in relative terms, easy through the removal of the need for dedicated communications in software.

One should also bear in mind that, although 3G networking was originally sold on the promise of video-calling, the reality is that the adoption of Internet protocols and integration of web browsers into smartphones has driven the development of mobile technologies far more than a single application. Allied to this is the fact the mobile phone has evolved to become a lifestyle device, used to access or share data on demand, rather than purely a communications device. Again, this suggests that the critical factor is not so much the original core functions of these devices as it is the "always available for ad-hoc use" nature of modern smartphones, which has led to them become lifestyle complements.

3 | DISCUSSION

Metaverse devices are, we argue, currently the equivalent of the web clients prior to 1995. They should be multi-protocol devices, because of the range of services with which they have to interact, but more importantly they are not bundled devices. They are add-ons, and often perceived as expensive, complicated and unwieldy with few new services available, which provide a compelling reason for their adoption.[3] Furthermore, because VR devices are designed to be immersive, they isolate the user from the surrounding real world, potentially creating hazards insofar as the user may not be aware of incidents occurring around them (e.g., fire alarms, phone calls, other people entering the room, etc.) but they also fail to provide the level of immersion that has been suggested in works of fiction ranging from William Gibson's vision of Cyberspace to the popular entertainment presentation of VR as being akin to teleporting into a new environment with full sensory immersion. AR devices, although potentially less intrusive, suffer from regulatory concerns around use whilst engaged in difficult tasks, such as driving (Kiss, 2013), and their ability to distract the user as well as privacy concerns about the inclusion of cameras and microphones which may be always on (Iqbal & Campbell, 2022). They also, we suggest, have the potential to provide assistance to criminals in "meat space" when combined with Machine Learning systems, which have been trained to provide information based on facial recognition, and are capable of profiling potential victims based on their appearance and actions.

Therefore, we suggest that, although the metaverse as described in the opening paragraphs of this paper has potential for end-point forensics (i.e., analysis of artifacts present on the interface devices may lead to discovery of interactions with or through the various services to which a VR device can connect), it is unlikely to be as ubiquitous as browser-based evidence until such time as an essential service (McGrath, 2003), only accessible by VR, drives uptake, or a major vendor chooses to make VR a bundled part of its offering, complementing the existing desktop in a way that provides significant benefits and leading to mass adoption. We suspect, however, that no large vendor is particularly motivated to do this because of the risk of regulatory action (Buhr et al., 2010), which would force them to make their platform more open to competition, thus reducing their return on investment and removing competitive advantage. Moreover, defining VR and AR as the metaverse proposes that the fundamental change lies in the way that services are presented to, and interacted with by, the user rather than, as our discussion suggests, the creation of new opportunities for interaction. Although VR and AR can provide a richer user experience, they do not fundamentally change the levels or types of connectivity between devices, or people, in the way that the inclusion of simpler dial-up networking did in 1995. Of the two, as we note above, AR may have more

immediately applicable benefits from criminals in the short-term, especially if AR tagging of people and objects in meatspace becomes widespread.

For this reason, we return to our definition of the metaverse as being an extension of the original vision of the web—that is, a larger collection of application layer protocols that can be accessed by multiple user interface layer applications and devices, many of which provide their functions by aggregating services under a common interface. The ability to investigate any of these clients, in the form of end-point forensic activity, produces initial information, which can then be corroborated or extended through understanding of the application layer protocols used and the information exchanged through the use of these protocols.

Consideration of the metaverse in this way also allows for the concept of the "digital twin" to be reconsidered. Rather than it necessarily being a rich virtual representation of an object or entity (Jones et al., 2020), the digital twin contains sufficient identification elements to enable it to be recognized as equivalent to the original for the purposes of some action in the metaverse, not necessarily restricted to visual recognition and/or manipulation by a human. This may, as is currently the case, be simply some form of secret token, or it may extend to a collection of tokens and behaviors that mimic the relevant properties of the original or provide sufficient information for identity to be adequately authenticated (Marshall & Tompsett, 2005). This is not a particularly new concept and there have been many instances of criminals creating false "digital twins" such as near-identical URLs, cloned websites and copied or subverted identities (e.g., email accounts, corporate logos, etc.) for their own purposes. Within the metaverse, we expect to see this continuing, with increasing use of Machine Learning used to replicate behavioral aspects, potentially with modification to interact with targets in a realistic way in order to prepare them to be victims of, or unwitting accomplices in, some criminal act.

The fediverse (Cohn & Mir, 2022) may provide additional opportunities for "digital cloning" to take place, especially if compromised or malevolent federated servers are connected and used to acquire data from digital twins as they move around the grid. This is an extension of current tactics used to acquire social media, and other credentials, through the use of fake login prompts and other technology-assisted social engineering methods (Box 2).

BOX 2 Apple enters the fray

Toward the end of this paper being drafted, Apple launched their "Vision Pro" VR/AR headset, with built-in operating system. From the perspective of these authors, while the fact that it is an Apple product means that it will be adopted by many loyal customers, this headset still suffers from most of the problems we outline above, namely:

- It is an intrusive device, tending to make its presence obvious to both user and observer.
- It seems to be intended to replace rather than complement existing general purpose computing technology and may suffer from key applications not being compatible with it until a significant time after launch, if a critical mass of users exists to drive the need for compatibility.
- It is, at the time of writing, too expensive to be bundled with other systems as a useful add-on for general use, and less attractive to the average domestic user who has already invested in other platforms.
- The inclusion of camera and microphones, required for the AR functionality and user interface, create the same questions about privacy and responsible use.
- The AR functions, if found to be used inappropriately by a significant number of users, will lead to regulatory intervention to restrict usage.
- It is an Apple device, and therefore likely to be restricted to their "walled garden," in some aspects at least, making it less likely to be adopted for business use in those industries, which traditionally, and for financial reasons, adopt other platforms.

As a step towards a new paradigm, it is an interesting development but may, as with the Newton (Homan, 2013; Trudeau, 1993), represent a first foray into something that needs more time to mature before becoming widely adopted. Shortly before the Apple announcement, reductions in staffing for VR projects within Meta and Google appeared to be underway, suggesting that a shift in focus may already be in progress (Roth, 2023).

4 | CONCLUSION

As the Council of the European Union's Analysis and Research team notes, in the introduction to its metaverse report (ART Analysis and Research Team, 2022):

> "Big if true...the Metaverse could well add an additional dimension to human experience. It could constitute an entirely new space offering limitless possibilities and the potential to change our lives. Alternatively, it could turn out to be something of an empty shell: a fantasy pushed by the social media industry to distract attention from some of their current difficulties."

The Metaverse, as an immersive virtual environment, does have the potential to facilitate crime in much the same way as other Internet technologies, not least because it is built upon those technologies. Forensic examination of devices, which provide the immersive experience at the enabler/mediator level in the communications model (Figure 2), do have the potential to provide information about the nature of criminal acts, similar to the information extracted from mobile handsets, tablets, or personal computers, but it will be constrained by the device software's configuration and ability to record such information and may show only a limited view of the totality of the activity that was involved. Given that most crimes are identified by the victims, this leads to a situation where the devices to be examined are primarily those of the victims, leading to a somewhat biased victimological view of online crimes.

Thus, an end-point device view of the Metaverse is likely to be restrictive, if not biased, and it may be more fruitful to expand the view to consider it more holistically, with the immersive interactive experience being treated as just one facet of the wider metaverse, albeit with a useful role to play in dictating how the user experienced the metaverse. This wider metaverse already exists, as we have discussed above, in the collection of services already available in Cyberspace and those preparing to develop investigative methods and tools should bear in mind that, ultimately, the data behind the immersive experience may prove to be a richer source of evidence than that captured by end-point devices alone. This is especially true when one considers the distributed nature of some services, the potential for machine learning systems to be developed to assist in, or even commission, criminal activities, and for human perception-augmenting devices (e.g., AR glasses or AR apps on mobile phones) to allow components of the metaverse to be used to assist activities in the physical world.

As we proposed at the start of this discussion, the metaverse is not new. The metaverse as proposed by Interpol and Europol is, rather, a more refined way of experiencing a metaverse that was created when the first two computers were connected together in 1965, or 1983 if the reader wishes to constrain it to IP-based networks (Science + Media Museum, 2020). Since that date, the metaverse has expanded and evolved into the agglomeration of higher-level protocols and presentation/interaction software that we see today. The frontier may have grown as a result of this, but fundamentally, it is no longer a new frontier (Box 2).

AUTHOR CONTRIBUTIONS

Angus McKenzie Marshall: Conceptualization (lead); investigation (lead); methodology (lead); project administration (lead); writing – original draft (lead); writing – review and editing (lead). **Brian Charles Tompsett:** Investigation (supporting); methodology (supporting); writing – review and editing (supporting).

CONFLICT OF INTEREST STATEMENT

The authors declare no conflicts of interest.

DATA AVAILABILITY STATEMENT

"Data sharing is not applicable to this article as no new data were created or analyzed in this study.

ORCID

Angus McKenzie Marshall https://orcid.org/0000-0003-2074-5053
Brian Charles Tompsett https://orcid.org/0000-0002-2566-9339

RELATED WIREs ARTICLES

Can Zoom video conferencing tool be misused for real-time cybercrime?

ENDNOTES

[1] Aka the "real world"—meatspace is a term coined by J. P. Barlow and popularized in William Gibson's "Cyberpunk" novels.

[2] In this document, we tend to use the term "policing" as short-hand for any public protection activity, including combatting disinformation and breaches of local rules associated with particular services.

[3] At this point, the authors would have wished to include discussion of 3D cinema and TV technologies. These seem to experience periodic surges in popularity, followed by rapid decline into near-obsolescence, but we have been unable to find suitable peer-reviewed studies of this phenomenon.

REFERENCES

Science + Media Museum. (2020, December 3). A short history of the internet. https://www.scienceandmediamuseum.org.uk/objects-and-stories/short-history-internet

ART Analysis and Research Team. (2022). *Metaverse—Virtual world, real challenges*. Council of the European Union https://www.consilium.europa.eu/media/54987/metaverse-paper-9-march-2022.pdf

Ballenson, J. (2021). Nonverbal Overload: A theoretical argument for the causes of zoom fatigue. *Technology, Mind and Behaviour*, *2*(1). https://doi.org/10.1037/tmb0000030

Berners-Lee, T. (1989). *Information management: A proposal*. CERN https://www.w3.org/History/1989/proposal.html

Bown, J., White, E., & Boopalan, A. (2017). Looking for the ultimate display: A brief history of virtual reality. In J. Gackenbach & J. Bown (Eds.), *Boundaries of self and reality* (pp. 239–259). Academic Press. https://doi.org/10.1016/B978-0-12-804157-4.00012-8

Buhr, C.-C., Bulst, F. W., Foucault, J., & Kramler, T. (2010, November). The commission's decision in the Microsoft internet explorer. *Competition Policy Newsletter*, *1*, 37–40. https://ec.europa.eu/competition/publications/cpn/2010_1_12.pdf

Cohn, C., & Mir, R. (2022). *The fediverse could Be awesome (if we don't screw it up)*. Electronic Frontier Foundation (EFF) https://www.eff.org/deeplinks/2022/11/fediverse-could-be-awesome-if-we-dont-screw-it

Dash, A. (2020, August 25). What Windows 95 changed. https://www.anildash.com/2020/08/25/what-windows-95-changed/

Engelbart, D. C., & Lehtman, H. (1988, December). Working Togethr. *BYTE Magazine* (pp. 245–252).

Europol. (2023). *Policing the metaverse: What law enforcement needs to know, an obervatory report from the Europol Innovation Lab*. Publications Office of the European Union https://www.europol.europa.eu/publications-events/publications/policing-in-metaverse-what-law-enforcement-needs-to-know

Furnell, S., & Spafford, E. H. (2019). The Morris worm at 30. *ITNOW*, *61*(1), 21–33.

Hess, J., & Mutterlein, T. (2017). Immersion, presence, interactivity: Towards a joint understanding of factors influiencing virtual reality acceptance and use. Americas Conference on Information Systems. https://api.semanticscholar.org/CorpusID:20951134

Hoffman, D. L., & Novak, T. P. (1994). Wanted: Net census. *Wired*, *2*, 11.

Hoffman, D. L., Novak, T. P., & Chatterjee, P. (1995). Commercial scenarios for the web: Opportunities and challenges. *Journal of Computer-Mediated Communication*, *1*(3). https://academic.oup.com/jcmc/article/1/3/JCMC136/4584317

Homan, M. (2013, August 5). Remember the apple Newton's prophetic failure and lasting impact. WIRED. https://www.wired.com/2013/08/remembering-the-apple-newtons-prophetic-failure-and-lasting-ideals/

Interpol. (2023). *Technology assessment report on metaverse*. Interpol https://www.interpol.int/en/News-and-Events/News/2022/INTERPOL-launches-first-global-police-Metaverse

Iqbal, M. Z., & Campbell, A. G. (2022, April 4). Adopting smart glasses responsibly:Potential benefits, ethical, and privacy concerns with ray-ban stories. *AI and Ethics*, *3*, 325–327. https://doi.org/10.1007/s43681-022-00155-7

Jones, D., Snider, C., Yon, J., & Hicks, B. (2020, May). Characterising the digital twin: A systematic literature review. *CIRP Journal of Manufacturing Science and Technology*, *29*(Part A), 36–52. https://doi.org/10.1016/j.cirpj.2020.02.002

Kantor, B., & Lapsley, P. (1986, February). *RFC 977: Network news transfer protocol*. Engineering Task Force (IETF) https://datatracker.ietf.org/doc/html/rfc977

Kiss, J. (2013, July 31). *UK set to ban Google glass for drivers*. The Guardian https://www.theguardian.com/technology/2013/jul/31/google-glass-drivers

Krueger, M. W. (1977). *Responsive environments. Proceedings of the Junbe 13–15, 1977 National Computer Conference (AFIPS'77) (pp. 423–433)*. Association for Computing Machinery. https://doi.org/10.1007/978-3-030-67822-7_2

Liu, Z., Xiang, Y., Shi, J., Gao, P., Wang, H., Xiao, X., Wen, B., Li, Q., & Hu, Y.-C. (2022). Make Web3.0 connected: A perspective from interoperability and programmability across blockchains. *IEEE Transactions on Dependable and Secure Computing*, *19*(5), 2965–2981. https://doi.org/10.1109/TDSC.2021.3079315

Malik, O. (2020). 25 years later, they should send windows 95 a thank you card. https://om.co/2020/08/31/25-years-later-the-should-send-windows-95-a-thank-you-card/

Markus, M. L. (1987). Toward a 'critical mass' theory of interactive media: Universal access, interdependence and diffusion. *Communication Research*, *14*, 491–511.

Marshall, A. (2015). IRQ: The power of words. In R. Isbell (Ed.), *Digital forensics magazine*. TR Media Ltd. https://www.researchgate.net/publication/301699090_IRQ_The_Power_of_Words

Marshall, A., & Clarkson, A. (2008). Future crimes and detection methods in cyberspace. *Measurement and Control*, *41*(8), 248–251. https://doi.org/10.1177/002029400804100803

Marshall, A. M. (2018). WhatsApp server-side media persistence. *Digital Investigation*, *25*, 114–115.

Marshall, A. M., & Miller, P. (2019). Casenote: mobile phone call data obfuscation & techniques for call correlation. *Digital Investigation*, *29*, 82–90.

Marshall, A. M., & Tompsett, B. C. (2005). Identity theft in an online world. *Computer Law and Security Review*, *21*(2), 128–137. https://doi.org/10.1016/j.clsr.2005.02.004

McCahill, M. P., & Anklesaria, F. X. (1994). Evolution of the internet gopher. In H. Maurer, C. Calude & A. Salomaa (Eds.), *J.UCS The Journal of Universal Computer Science* (pp. 235–246). Springer-Verlag. https://doi.org/10.1007/978-3-642-80350-5_23

McGrath, S. (2003, January 7). Spreadsheets finally yield their buried treasure. *Computerworld* https://www.computerworld.com/article/2784938/spreadsheets-finally-yield-their-buried-treasure.html

Morris, I. (2015, August 24). *Seven ways windows 95 changed the world*. Forbes.

Mott, M., Tang, J., Kane, S., Cutrell, E., & Morris, M. R. (2020). I just went into it assuming that I wouldn't be able to the full experience. In *Understanding the accessibility of virtual Teality for people with limited mobility. Proceedings of the 22nd international ACM SIGACCESS conference on computers and accessibility (ASSETS '20). Article 43* (pp. 1–13). ACM. https://doi.org/10.1145/3373625.3416998

Ritterbusch, G. D., & Teichmann, M. (2023). Defining the metaverse: A systematic literature review. *IEEE Access*, *11*, 12368–12377. https://doi.org/10.1109/ACCESS.2023.3241809

Roth, E. (2023, July 10). *Google's AR software leader is out over the company's 'unstable commitment and vision'*. Vox Media. https://www.theverge.com/2023/7/10/23790393/google-ar-software-leader-mark-lucovsky-project-iris

Saleem, J., Islam, R., & Kabir, M. (2022). The anonymity of the dark web: A survey. *IEEE Access*, *10*, 33628–33660.

Salter, M. (2017). *Crime, justice and social media*. Routledge.

Schofield, J. (2016). *NOMINET presents the story of the web: Celebrating 25 years of the world wide web*. NOMINET http://storyoftheweb.org.uk/report/storyoftheweb.pdf

Stoll, C. (1989). *The Cuckoo's egg: Tracking a spy through the maze of computer espionage*. Doubleday.

Sutherland, I. (1968). A head-mounted three dimensional display. *Proceedings of AFIPS 68* (pp. 757–764). Association for Computing Machinery.

Trudeau, G. (1993, August 27). Doonesbury. GoComics. https://www.gocomics.com/doonesbury/1993/08/27

Vertucci, R., D'Onofrio, S., Ricciardi, S., & Nino, M. D. (2023). History of augmented reality. In Y. Nee & S. Ong (Eds.), *Springer handbook of augmented reality*. Springer. https://doi.org/10.1145/1499402.1499476

Zakon, R. H. (2018, January 1). *Hobbes' Internet Timeline*, *25* https://www.zakon.org/robert/internet/timeline/

How to cite this article: Marshall, A. M., & Tompsett, B. C. (2023). The metaverse—Not a new frontier for crime. *WIREs Forensic Science*, e1505. https://doi.org/10.1002/wfs2.1505