EUROPOL

Policing in the metaverse: **what law enforcement needs to know**

An Observatory Report from the Europol Innovation Lab

POLICING IN THE METAVERSE: WHAT LAW ENFORCEMENT NEEDS TO KNOW
An Observatory Report from the Europol Innovation Lab

PDF | ISBN 978-92-95220-47-8 | ISSN 2600-5182 | DOI: 10.2813/81062 | QL-AS-22-002-EN-N

Luxembourg: Publications Office of the European Union, 2022

Cite this publication: Europol (2022), Policing in the metaverse: what law enforcement needs to know, an observatory report from the Europol Innovation Lab, Publications Office of the European Union, Luxembourg.

This publication and more information on Europol are available on the Internet.

www.europol.europa.eu

Contents

Foreword

Europol launched its Innovation Lab in 2019, to help keep Europol at the forefront of law enforcement innovation. I believe it is important for law enforcement agencies to anticipate changes to the reality in which they have to provide safety and security. That is why our Innovation Lab includes an Observatory function, to engage in strategic foresight and help law enforcement agencies to understand the implications of emerging technologies.

The metaverse will bring us new ways of interacting and whole new (virtual) worlds to live in, potentially transforming our lives, just as the internet has done in the last three decades. This report will undoubtedly help police chiefs, law enforcement agencies and policy makers to begin to grasp this new environment, so that they can begin to adapt and prepare for policing in the metaverse.

Catherine De Bolle
Executive Director of Europol

Introduction

The metaverse has been described as the next iteration of the internet.[1] As was the case with the emergence of the internet, we do not know what direction the metaverse is going to take. Moreover, like the internet, it will likely keep evolving periodically taking new directions. Keeping in mind that historically law enforcement was generally slower in developing capabilities for digitally committed crimes, we should as soon as possible begin preparing for the emergence of the metaverse from a law enforcement perspective.

With the recent launch of Meta's platform Horizon Worlds in France and Spain the company is bringing its immersive world or metaverse experience to Europe.[2] When Mark Zuckerberg announced[3] in October 2021 that Facebook would now be called Meta, it brought the concept of the metaverse to the public's attention. Google, Microsoft and many others are also making big investments in this technology.[4] With an expected EUR 1.6 trillion boost to the global economy by 2030[5] and with 25% of people expected to spend at least an hour daily in the Metaverse[6], it will certainly have an impact on the (in)security of citizens and be something law enforcement needs to be looking into.

To help make sense of the impact that metaverse and the technologies underpinning it may have on criminal activities and how the police will need to adapt to respond to new security needs of citizens, the Europol Innovation Lab organised an event on the metaverse for European law enforcement agencies in June 2022. During the event, academics from different fields of expertise shared the results of their research on human behaviours in digital environments, the developing economic ecosystems related to these environments and the metaverse. The company Meta shared their vision of and approach to the metaverse. Experts in law enforcement spoke about their experiences and thoughts on what challenges the metaverse may present in terms of security and discussed ways for the police to adapt its practices. The event was attended by over 120 representatives from law enforcement agencies from all over Europe. In a series of foresight exercises, the participants expressed a clear need for resources to help European police officers understand better the risks and opportunities posed by the metaverse and its related technologies.

1 Journal of Law and Technology, 'The Metaverse: Are We Prepared for the Dangers of This Digital Reality?', 2022, [accessed 24 August 2022], https://jolt.richmond.edu/2022/03/31/the-metaverse-are-we-prepared-for-the-dangers-of-this-digital-reality/.

2 Facebook, post by Mark Zuckerberg, 2022, [accessed 18 August 2022], https://www.facebook.com/photo/?fbid=10114625396809351&set=a.612287952871.

3 The New York Times, 'The Metaverse Is Mark Zuckerberg's Escape Hatch', 2021, [accessed 1 September 2022], https://www.nytimes.com/2021/10/29/technology/meta-facebook-zuckerberg.html

4 Make Use Of, 'These 8 Tech Giants Have Invested Big in The Metaverse', 2022, [accessed 1 September 2022], https://www.makeuseof.com/companies-investing-in-metaverse/

5 PWC, 'Virtual and augmented reality could deliver a £1.4trillion boost to the global economy by 2030 – PwC', 2020, [accessed 1 September 2022], https://www.pwc.com/id/en/media-centre/press-release/2020/english/virtual-and-augmented-reality-could-deliver-a-p1-4trillion-boost.html

6 Gartner, 'Gartner Predicts 25% of People Will Spend At Least One Hour Per Day in the Metaverse by 2026', 2022, [accessed 1 September 2022], https://www.gartner.com/en/newsroom/press-releases/2022-02-07-gartner-predicts-25-percent-of-people-will-spend-at-least-one-hour-per-day-in-the-metaverse-by-2026.

This report aims at bringing together all the information gathered during this event. It provides a first, law enforcement-centric outlook at current developments, potential implications for law enforcement, as well as key recommendations as to what the law enforcement community could do to prepare for the future.

The first part presents the concept of immersive worlds and the technologies underpinning it, such as virtual and mixed reality, web3 and blockchain. In the second part, the report explores how the metaverse can be abused in specific crime areas such as financial crime, online abuse and harassment, radicalisation, mass surveillance and disinformation. But the metaverse could also present opportunities for the police, not only from an investigation perspective but also to engage more closely with the public it serves or for training purposes. The third part of the report focuses on those. The final part of the report will explore best practices of building police presence online and will provide recommendations for police forces around the world to start thinking about their online policing strategies for the future.

The Europol Innovation Lab is especially grateful to Mrs. Manon den Dunnen from the Dutch National Police for sharing her inspiring thoughts about our changing reality, and to Ms. Kjersti Rønholt from the Criminal Investigation Service (Kripos) of the Norwegian Police for her pioneering work in establishing police presence in digital environments. We would also like to thank our academic contributors: Professor David Reid from Liverpool Hope University, Professor Shane Johnson from University College London, and Anna-Verena Nosthoff and Felix Maschewski from the Data Politics Lab at Humboldt University Berlin. Lastly, we are grateful to our colleagues in Europol at the European Cybercrime Centre (EC3) and the EU Internet Referral Unit, as well as to the Office of the EU Counter Terrorism Coordinator (EU CTC) for their valuable contributions.

What is the Metaverse?

The basics of the metaverse

The term metaverse was first coined in 1992 by the author Neal Stephenson in his science fiction novel Snow Crash. Just as the metaverse was science fiction in 1992, today a 'real' metaverse still does not yet exist. The metaverse is often described as a hypothetical iteration of the internet as a single, universal virtual world that presents the user with an immersive experience that feels 'real', usually through the use of a headset. In its very recent definition, it can blur the lines between the physical and virtual world to create a single blended, extended or mixed reality. As a result, the metaverse is now just focused on virtual reality (VR), but is increasingly being defined in terms of augmented reality (AR) or extended or mixed reality (XR).

Since then the word has been frequently used to present a variety of different visions on what a shared, immersive, and virtual world might look like. From the grand visions presented, it may hold great promise to allow people to enjoy experiences free of physical limitations and have more autonomy because of decentralised technology. In practice it will be shaped by companies building and using it, and by how the people use the options provided by the technology. Together that will determine whether it will be a utopian place - or one rife with crime and abuse.

Proposed applications for metaverse technology go beyond gaming, and include improving work productivity, interactive learning environments, e-commerce, real estate and fashion. It seems likely that most metaverse(s) will include a digital economy, where users can create, purchase, and sell goods.

In the more idealistic and holistic vision of the metaverse, it is interoperable, allowing people to take virtual items like clothes or cars from one platform to another. Right now, most platforms have virtual identities, avatars, and inventories that are tied to a particular platform. However, a metaverse might allow one to create a persona that can be taken everywhere in the metaverse with all its characteristics and your belongings. To date this has remained very limited however; as most platforms demand you create an account specific for their platform.

In visions like that of Meta, the metaverse is considered to be the evolution of internet[7], or an embodied internet. Other visions include immersive offline experiences that enable users to experience a different reality, or a combination of the physical and virtual world in a type of mixed reality. An important factor in this is the idea of so-called 'digital twins', which provide a model of offline entities that digitally represents them as accurately as possible, often providing real-time information from sensors. This will allow further integration of the virtual and physical worlds by representing the latter in real-time in the former, autonomously. Thus, integration of

7 Meta, 'Connect 2021: Our vision for the metaverse', 2021, [accessed 25 August 2022], https://tech.fb.com/ar-vr/2021/10/connect-2021-our-vision-for-the-metaverse/

the physical and virtual worlds goes both ways, blending both worlds.

Examples of this are Seoul's recent announcement to provide many of its access to public services via the metaverse[8] is one such example. Even entire countries, such as Singapore, are investing heavily in providing digital twins.[9] An instance of avatar work can be found at a café in Tokyo, where paralysed people control robot waiters remotely. The waiter can see the café and the people in it through the robot, and control it to wait the tables and start a conversation. This enables people to do work they otherwise could not do by using a physical avatar.[10]

The metaverse and application of related technology are envisioned in many different ways, but they all share the concept of immersion in a (partial) virtual world, bringing experiences from the physical world to the virtual realm. Even an Internet of Senses[11] and implanted chips for full immersion[12] have been suggested. With such interfaces, increasingly one may not be able to tell the virtual from the physical.

We cannot know if there will be a single 'metaverse', a metaverse of metaverses (a multiverse), or if it turns out to be just an appealing term to encompass different technological developments undertaken by big companies. However, as the metaverse paper by the Council of the European Union's Analysis and Research Team notes, "As is the case for most of the tech sector, the product itself creates the need."[13] Moreover, with the combined market for VR and AR estimated to be worth EUR 4 billion, a number forecasted to grow to EUR 36 billion[14], many companies are investing in metaverse technology. While this is not a guarantee for adoption of the metaverse, the sizeable investments from a broad range of companies makes widespread adoption, of at least some aspects, more likely. Therefore, a closer look at what the technology means for law enforcement is warranted.

8 ICT Network News, 'Seoul to use metaverse platform to deliver public services', 2021, [accessed 7 September 2022], https://www.ict-nn.com/seoul-to-use-metaverse-platform-to-deliver-public-services/

9 Venture Beat, 'How Singapore created the first country-scale digital twin', 2022, [accessed 7 September 2022], https://venturebeat.com/business/how-singapore-created-the-first-country-scale-digital-twin/

10 Barista Magazine Online, DAWN Avatar: A Robot-Run Café Made for Inclusion in Tokyo', 2021, [accessed 5 September 2022], https://www.baristamagazine.com/dawn-avatar-a-robot-run-cafe-made-for-inclusion-in-tokyo/

11 Ericsson, 'Internet of senses', [accessed 25 August 2022], https://www.ericsson.com/en/6g/internet-of-senses.

12 Futurism, 'Elon Musk Says the Metaverse Sucks and Neuralink Will Be Better', 2021, [accessed 17 August 2022], https://futurism.com/elon-musk-metaverse-sucks-neuralink-better/.

13 Council of the European Union, 'Metaverse – Virtual World, Real Challenges', 2022, page 5, [accessed 26 July 2022], https://www.consilium.europa.eu/media/54987/metaverse-paper-9-march-2022.pdf.

14 IDC, 'Spend on Emerging Device Categories – including Wearables, AR/VR Headsets, and Smart Home – Will See Continued Robust Growth, According to IDC', 2021, [accessed 18 August 2022], https://www.idc.com/getdoc.jsp?containerId=prUS48284221

Current state of play

The concept of virtual worlds is not new, and technology like virtual and augmented reality has been around for a while. This will all have to be further developed and supported by additional technology to present a metaverse as immersive as it is currently envisaged. Considering this, there are some examples of metaverse-like experiences, mostly in gaming. These games may give us an idea of how a metaverse could work, but they do not live up to the immersive and interoperable character described by advocates of the metaverse.

The earliest examples of a virtual world may have been multi-user dungeons dating back to the 1970s.[15] Players would be presented with a text-based description of the environment and events, and would interact with the world and other players through text. A prominent example of a more visual experience is Second Life. This is often referred to as an early example for its replication of all aspects of life, launching back in 2003.[16] Companies opened offices and bands like U2 gave concerts there, but it never broke through to attract the mass following like social media platforms such as Facebook did.[17] The two closest, and most often referred to examples of a metaverse, are Fortnite and Roblox.[18] Fortnite is a battle royale videogame with a 3D virtual world where players can engage in non-game interactions such as concerts, whereas Roblox is a platform where people can create their own experiences or mini-games and share these with other users, free or for a fee, and use their own avatar in all of these experiences.[19] Both games have tens of millions of players.

These examples are mostly experienced through computers or smartphones. Depending on the level of immersiveness, accessing the metaverse 'proper' will require some kind of headset for virtual or augmented reality applications.[20] VR refers to instances where technology is used to present a virtual world, which is experienced as reality whereas XR (MR/AR) presents new information as an overlay on top of the physical world. New devices are developing at an incredibly quick pace; many see the new generation of XR devices as the natural successor to the laptop or mobile phone.

15 Rappler, 'The metaverse isn't here yet, but it already has a long history', 2022, [accessed 5 September 2022], https://www.rappler.com/technology/features/metaverse-not-here-yet-but-has-long-history/

16 Make Use Of, 'What Is Second Life? A Brief History of the Metaverse', 2022, [accessed 2 September 2022], https://www.makeuseof.com/what-is-second-life-history-metaverse/.

17 IEEE Spectrum, 'What Can the Metaverse Learn From Second Life?', 2021, [accessed 3 September 2022], https://spectrum.ieee.org/metaverse-second-life

18 OMDIA, 'Roblox dethrones Fortnite in Omdia's new Metaverse Games Benchmark ', 2022, [accessed 18 August 2022], https://omdia.tech.informa.com/pr/2022-jul/roblox-dethrones-fortnite-in-omdias-new-metaverse-games-benchmark

19 BirminghamLive, 'What is a Metaverse, why are Fortnite and Robolox building one?', 2021, [accessed 17 August 2022], https://www.birminghammail.co.uk/sport/gaming/what-metaverse-fortnite-robolox-building-21974498

20 Medium, 'The Technology of the Metaverse, It's Not Just VR', 2020, [accessed 25 August 2022], https://medium.com/swlh/the-technology-of-the-metaverse-its-not-just-vr-78fb3c603fe9.

Technology powering metaverses

While some virtual and augmented reality technology has been around for some time, it is still under heavy development and is supported by many different technologies, like spatial computing, sensors, haptics and location services.[21] As with XR and VR, metaverse creations will rely on extended hardware and software to access the platform, as well as accompanying technology to facilitate the platforms. The technology known as Web3 is often seen as an enabling technology for the metaverse. This chapter will provide an explanation of this technology to help understand how this all comes together in creating a metaverse.

Headsets are used for VR applications and the most immersive XR applications. A headset needs to be both comfortable and a powerful enough computer to be able to present and control the metaverse experience in the sense that it will present a life-like reality in which we feel fully immersed. So far, the development and general consumer adoption of these extended reality applications has been held back by price and the limitations of such headsets, since the wireless networking speed is too low and the computing power required can make them uncomfortable or necessitate wired connections that limit users' movement.[22] Moreover, they often cause nausea, due to motion sickness, when used for some time.[23]

Another issue, mainly for virtual reality, is limitation of physical user movement. To provide a good experience for moving around in VR, a big empty space is needed to avoid obstacles such as walls or nearby objects. To allow for better interaction with (and more convincing creation of) virtual environments, advances in spatial computing will be the main deciding factor. This will be accompanied by improvements in location services to provide the user's location in physical space as accurately as possible.[24]

To improve the immersion of the experience, new interfaces like haptics, interaction and feedback through sensory suits or even neural links are being suggested. All this technology is still in development.[25] In particular new VR or XR platforms are attracting a lot of attention from developers such as Meta, Apple and Google. Such devices are seen as not only a new type of computer, but as

21 McKinsey & Company, 'Technology Trends Outlook 2022', 2022, [accessed 7 September 2022], https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/the%20top%20trends%20in%20tech%202022/mckinsey-tech-trends-outlook-2022-research-overview.pdf

22 TechRadar, 'This Oculus VR headset could feature lifelike resolution – here's why that matters ', 2021, [accessed 23 August 2022], https://www.techradar.com/uk/news/this-oculus-vr-headset-could-feature-lifelike-resolution-heres-why-that-matters.

23 Space.com, 'What causes motion sickness in VR, and how can you avoid it?', 2021, [accessed 5 September 2022], https://www.space.com/motion-sickness-in-vr

24 McKinsey & Company, 'Technology Trends Outlook 2022', 2022, [accessed 7 September 2022], https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/the%20top%20trends%20in%20tech%202022/mckinsey-tech-trends-outlook-2022-research-overview.pdf

25 Financial Times, 'Investors gear up for 'gold rush' in metaverse hardware', 2022, [accessed 2 September], https://www.ft.com/content/51351f23-63b8-458c-9ee2-a7cbda43c287

a fundamentally new computing paradigm; this is called spatial computing.

For metaverse experiences, software is needed to allow devices to provide access to the metaverse and to create and serve the experiences on these platforms. The computational requirements needed to provide realistic simulation of imagined worlds in the metaverse, with social interactions and large crowds, are quite demanding. Simultaneously, these devices need to monitor the user and their surroundings, adding to the demands on the hardware. However, advances in computer processors meet these computational requirements.

Another limitation to development is the absence of a set of technical standards, like W3C for web development. With every major company developing their own software, it is difficult to navigate this space as a developer and the interoperability of metaverses lies far ahead. Moreover, with the propriety of the code as we have seen it on social media, it will be difficult to achieve transparency and be certain the privacy of a user is guaranteed.

There are a few attempts at standardisation, like universal scene description for 3D computer graphics[26] and OpenXR for accessing VR and AR devices.[27] Major online service providers are still developing for their own platforms for now;[28] however cross-platform compatibility is becoming more and more common. For example, Nvidia's Omniverse platform can use its proprietary version of universal scene description, as can the Unity engine.

A good example of this is provided by WebXR. This is an open protocol designed to connect the different VR or metaverse platforms through the use of a browser. This allows a user to connect different platforms to the metaverse from a browser. As such it opens facilitates the idea of interoperability from one environment to another.[29]

Web3

Web3 is the term that is used for the next iteration of the internet, based on decentralisation, privacy and anonymity, with users and creators in charge of the internet and their data. Decentralisation in the Web3 is achieved using protocols like peer-to-peer (p2p) and blockchain technology. These decentralised services may have severe implications for the attribution of online crime as well as securing digital evidence of such crimes.

26 NVidia, 'Universal Scene Description Key to Shared Metaverse, GTC Panelists Say', 2021, [accessed 23 August 2022], https://blogs.nvidia.com/blog/2021/04/27/usd-metaverse-gtc/.

27 Steam, 'Introducing SteamVR 1.16', 2021, [accessed 26 August 2022], https://store.steampowered.com/news/app/250820/view/3044967019267211914

28 News18, 'Meta and Other Tech Giants Form Metaverse Standards Body, Apple Missing ', 2022, [accessed 24 August 2022], https://www.news18.com/news/tech/meta-and-other-tech-giants-form-metaverse-standards-body-apple-missing-5419855.html

29 VentureBeat, 'A primer on the Metaverse: The next iteration of the Internet', 2017, [accessed 24 August 2022], https://venturebeat.com/arvr/a-primer-on-the-metaverse-the-next-iteration-of-the-internet/.

Currently multiple projects combine blockchain and p2p technologies to provide services like gaming content, Non-fungible Tokens (NFTs) (which can be seen as proof of ownership on the blockchain), or storage solutions for media sharing. This is already-existing technology that may be used for the development of the metaverse and be further developed to accommodate the specific needs of metaverse technology.

While this technology may provide a decentralised internet, the technology is being taken up by big corporations to support their platforms too, leading to centralised services.

Blockchain

Use of the blockchain has been suggested as a means to provide the technology to allow users to take an avatar and assets from one metaverse to the next. Moreover, cryptocurrency is expected to play an important role in economic activity in the metaverse.[30]

Blockchain technology is based on having a record of cryptographically linked blocks. Every change results in the creation of a new block linked to previous blocks, creating a chain. This chain means no single record can be altered without altering all following blocks as well. Implementing the blockchain as a public distributed ledger means all records are public and any change is verified by several nodes in the network, creating additional safeguards of the integrity of the data on the blockchain.

Blockchain technology is most commonly known for its implementation for cryptocurrencies like Bitcoin and Ethereum. The blockchain provides a record of all transactions or changes made to a record and any transaction or change is checked by multiple different sources guaranteeing the validity of all changes. This may be useful for proof of ownership or validation of certificates. It is usually implemented to contain references to information, but it could be used to transfer the data itself as well.

Use of the blockchain has been proposed as a way to facilitate the interoperability of different metaverse platforms. In this case the records would contain all relevant information on the user's avatar, like attributes and possessions. By consulting the blockchain all platforms would find the same information on the user. That way users may appear the same on all these platforms (i.e. outfits and goods, but also metadata on the user) and thus be enabled to carry one identity across all platforms.

30 Citi GPS, 'METAVERSE AND MONEY', 2022, [accessed 2 September], https://icg.citi.com/icghome/what-we-think/citigps/insights/metaverse-and-money_20220330

Adverse use and crime in the metaverse

As with blockchain mentioned above, new technology will always provide new attack vectors for criminals. Bad actors will have new chances to take advantages of weaknesses in these new technologies from XR to interface devices as companies compete to define the metaverse market. Making it all the more important to call for safety by design.[31]

Just as with the early years of the internet, we cannot know exactly in which ways metaverse-native crimes or the metaverse version of cybercrimes may occur. We can be certain, however, that like the development of the internet, as the metaverse develops it will open up different opportunities for criminal activity. With Roblox rising to the 8th place as most imitated brand in phishing attempts according to last year's Q4 2021 brand phishing report, metaverse applications have certainly caught the attention of criminals.[32] Knowing Roblox is played most by children, 67% is under 16,[33] makes this all the more worrying.

Ransomware-type attacks may be particularly effective on metaverse devices. Considering the increased importance of digital assets in the metaverse, losing access to them may be particularly debilitating. If this is loss is in XR, where the virtual is blended with the real world, then this loss may have even greater consequences.

We will explore how the metaverse could potentially be used in some specific crime areas, to present a first glance at how the metaverse could affect law enforcement.

Identity

Increasing adoption and functionality of metaverse technology means digital identities, and access to them, will become more valuable. As the virtual representation of users in the metaverse becomes more realistic and permanent, this provides opportunities to convincingly copy user appearance (so called deepfakes). With more advanced ways to interact with the system by using different sensors, eye tracking, face tracking and haptics for instance, there will be far more detailed biometric information about individual users. That information will allow criminals to even more convincingly impersonate and steal someone's identity. Moreover, this information may be used to manipulate users in a far more nuanced, but far more effective way than is possible at present on the internet.

This creates issues of trust in the identity of the 'people' in the metaverse; how can you be sure of who you are actually speaking

31 Forbes, 'Metaverse As The New Attack Vector And Other Security Headlines To Come In 2022', 2022, [accessed 1 September 2022], https://www.forbes.com/sites/forbestechcouncil/2022/02/15/metaverse-as-the-new-attack-vector-and-other-security-headlines-to-come-in-2022/

32 CheckPoint, 'DHL Replaces Microsoft as Most Imitated Brand in Phishing Attempts in Q4 2021', 2022, [accessed 1 September 2022], https://blog.checkpoint.com/2022/01/17/dhl-replaces-microsoft-as-most-imitated-brand-in-phishing-attempts-in-q4-2021/.

33 Backlinko, 'Roblox User and Growth Stats 2022', 2022, [accessed 16 September 2022], https://backlinko.com/roblox-users.

to? Can AI be used to process what you are looking at, how you feel, or how you interact with people, and can this be used to influence people? This is, of course, an issue on the internet in general already, but metaverse applications, because of the significant increase in the amount of valuable biometric information it can gather, will present vastly more problems in this regard.

At the same time, there is the matter of who owns the user's virtual identity. If the owner of the platform claims ownership of all user-generated data, including any intellectual property created through their platform, this could extend to user avatars or representations on it. The more detailed that data becomes and the more closely that avatar resembles and represents the actual user, the more this becomes a question of who owns the user's identity, the biometric and spatial information that the user provides to the system.

A person's identity is defined by more than the appearance or avatar the user has. A user generates data through interactions with the platform. That data may become so detailed it may feel like a very accurate representation of the user's identity. Deep insight into desires and actions may define a user in practice. Knowing all small mannerisms of a user and where the user's eyes go to unconsciously, for instance, may be more defining that the exact look of an avatar. Would a platform then be able to sell or duplicate this virtual identity by virtue of owning the rights to the user's avatar or data? And what happens when criminals extract this data and user profiles?

Criminals have already been selling digital fingerprints on the dark web, which imitates the user's device's characteristics and behaviour. This allows a user of the service to use a browser plugin to imitate a victim's digital fingerprint for the purposes of fooling authentication systems.[34] With the very detailed information possibly gathered from users of the metaverse such exploits would become harder to fight. These could even be used to generate synthetic identities with all the depth of a person by adding a behavioural layer to deepfakes.

That would certainly create opportunities for abuse of your identity, or to influence your actions. With metaverse applications detecting unconscious signals, it may be able to present information to influence your decisions before you are even aware of it. Moreover, if the detailed personal information were used convincingly to imitate a person, this would make it very hard for law enforcement to know who the user is. This makes a very strong identification, or know your customer (KYC), procedure very important for metaverse platforms, in order to prevent identity theft and provide trust between users, as well as provide law enforcement with the means to investigate crimes committed on the platform.

34 CreditUnionTimes, 'The Rise of Digital Fingerprints in the Dark Marketplace Threatens Identities', 2019, [accessed 1 September 2022], https://www.cutimes.com/2019/08/28/the-rise-of-digital-fingerprints-in-the-dark-marketplace-threatens-identities/.

The generation of very detailed biometric data may be inescapable, as it is required to provide the life-like immersive experience of the metaverse. The question will be how the platforms handle this kind of data, in what ways is it processed and stored, and what safeguards are implemented to prevent the harvesting of this information by third parties. It will remain to be seen how well the implementation of these platforms conform to the GDPR.[35]

Criminals may also impersonate brands as well as people. This is a particularly common practice for phishing. With these attempts bad actors create emails to convince their victims these are legitimate emails from a certain brand to make them download something or click a link and thereby allow them to extract personal information such as account or banking details. In the metaverse, this might even be done with entire fake stores the user may just walk past and be convinced by the storefront. As more people start to use the metaverse, we should expect to see an increase of brand phishing related to and in the metaverse.[36]

Financial: money laundering, scams

Money and value may take different forms in the metaverse. While NFTs may allow for proof of ownership of digital goods, transactions in the metaverse may be facilitated by a range of different cryptocurrencies depending on the platforms involved, and fiat money is likely to persist as a means of entry from the regular to the metaverse economy.

For the economic aspect of the metaverse, it will be essential for users to be able to make payments easily and quickly. It will be important to keep the costs of transfers low since most transactions will be of small value. This means that, alongside our usual fiat money and the big cryptocurrencies we now know, it is likely to see the further implementation of platform-specific currencies and other decentralised cryptocurrencies.[37] Following these transactions will require knowledge of decentralised finance, the different blockchain implementations as well as familiarity with a range of different forms of digital currency.

The more one learns about metaverse plans from major players like Epic Games and Meta, the more it seems that anti-money laundering (AML) and know your customer (KYC) protections will be as important as they are in the real world. In a space populated by virtual businesses, selling virtual goods to avatars will require virtual money. This provides opportunities to transfer money

35 Agencia Española de Protección de Datos, 'Metaverse and Privacy', 2022, [accessed 6 September 2022], https://www.aepd.es/en/prensa-y-comunicacion/blog/metaverse-and-privacy

36 AIM, 'Fighting cybercrime in metaverse', 2022, [accessed 6 September 2022], https://analyticsindiamag.com/fighting-cybercrime-in-metaverse/

37 Citi GPS , 'Metaverse and Money: Decrypting the Future', 2022, [accessed 01 September 2022], https://icg.citi.com/icghome/what-we-think/citigps/insights/metaverse-and-money_20220330.

across borders in a way that is more difficult for the authorities to monitor.[38]

Cryptocurrencies are already being employed for purposes of money laundering and facilitating criminal money transfers.[39] This is expected to grow with further development adoption of cryptocurrencies. The possibilities for anonymous use of cryptocurrencies will make it difficult for law enforcement to detect these crimes.

The world of NFTs is rife with frauds, as well as misappropriation of other people's assets.[40] An NFT is a proof of ownership recorded on the blockchain and therefore unique and guaranteed to be so by the blockchain it is on. There are, however, ways to sell an NFT multiple times, using sufficiently different smart contracts or offering it on another blockchain. A seller does not even need to own what they offer to sell it as an NFT. While big marketplaces would presume to verify ownership, this is not practically possible because of the sheer number of NFTs being offered. The result is a situation where as many as 80% of NFTs created with OpenSea's minting tool are estimated to be illegitimate.[41] Additionally, while many NFTs are being offered by anonymous identities, it is difficult for legitimate creators of such virtual goods to establish their right of ownership. For prevention purposes, law enforcement agencies need to be aware of future NFT developments and future exploitations of the technology as they evolve.

Harassment and (child) abuse and exploitation

Harassment on the internet is already a significant issue, with as many as 58% of girls in an international 2020 Plan International survey having experienced online harassment.[42] Law enforcement should therefore expect this kind of behaviour to exist in the metaverse, with the potential for it to be even more damaging to the victim. In 2007, one avatar in Second Life allegedly raped another. A number of internet bloggers dismissed the simulated attack as nothing more than digital fiction, but police in Belgium opened an investigation against the perpetrator.[43] More recently, a woman

38 Reuters, 'UK group urges real-life treatment for virtual cash', 2007, [accessed 21 September 2022], https://www.reuters.com/article/us-britain-secondlife-idUSL146725220070514.

39 Europol, 'Cryptocurrencies: tracing the evolution of criminal finances', 2022, [accessed 31 August 2022], https://www.europol.europa.eu/publications-events/publications/cryptocurrencies-tracing-evolution-of-criminal-finances.

40 Gizmodo, 'Nearly All NFTs Created With OpenSea's Free Minting Tool Are Fake, Plagiarized, or Spam', 2022, [accessed 21 September 2022], https://gizmodo.com/nearly-all-nfts-created-with-opensea-s-free-minting-too-1848445234.

41 Engadget, 'Over 80 percent of NFTs minted for free on OpenSea are fake, plagiarized or spam', 2022, [accessed 31 August 2022], https://www.engadget.com/opensea-free-minting-tool-220008042.html.

42 PLAN International, 'Online harassment is silencing girls: the EU and its Member States can do more and better', 2020, [accessed 3 September 2022], https://plan-international.org/eu/blog/2020/11/25/online-harassment/.

43 WIRED, 'Virtual Rape Is Traumatic, but Is It a Crime?', 2007, [accessed 29 August], https://www.wired.com/2007/05/sexdrive-0504/

described how she was “virtually gang raped” within 60 seconds of joining Meta’s Venues.[44]

The woman described the aforementioned incident as rape. These kinds of virtual experiences pose serious questions about the applicability of current legislation. Rape requires physical contact, while by definition an avatar is virtual. However, as the embodied internet is one of the ways of describing the metaverse, one can imagine that, as the technology gets more sophisticated, this crude delineation between physical and virtual will become increasingly problematic. As these experiences become more embodied, start to feel more real, we will have to decide at which point virtual experiences will be equally impactful as those of the physical realm.[45] It will be important to have a clear idea of what is to be considered criminal behaviour in the metaverse and to have matching laws to provide the means to prosecute these transgressions.

While monitoring behaviour in the metaverse, it is important to look for new forms of harassment as well. If we were to have one (virtual) identity in the metaverse and all interactions in this metaverse are based on blockchain, this might make it possible to follow everything someone does based on one interaction with them - providing valuable information for stalkers or extortionists. This could also be used to send unwanted content. It is possible to send anyone an NFT or message on the blockchain, but once it is on the blockchain there is no way for anyone to remove it; this will mean any harassment may indefinitely show up if people look into your blockchain, blocking any way out of that abuse.[46]

Current iterations of the metaverse show how these may be dangerous for children. At the moment, there is no (effective) age rating of experiences spaces in the metaverse may offer. In the VRChat social virtual reality experience platform, users encountered strip clubs and children were exposed to harmful experiences.[47] Meanwhile in Roblox, people create sex ‘condos‘ where people talk about sex and make their avatars have virtual sex.[48] This may not be in line with the platforms’ policies, but children can be confronted with these experiences nonetheless. The platforms providing these services will have to provide a safe environment for children and provide safeguards against these experiences, by moderating content and behaviour that goes against their terms of use. Finding a way to effectively protect children from seeing harmful (sexual) content will be essential for a safe and positive experience for them.

44 Medium, ‘Reality or Fiction?’, 2021, [accessed 29 August], https://medium.com/kabuni/fiction-vs-non-fiction-98aa0098f3b0.

45 WIRED, ‘What Should Be Considered a Crime in the Metaverse’, 2022, [accessed 20 July 2022], https://www.wired.com/story/crime-metaverse-virtual-reality/.

46 Molly White, ‘Abuse and harassment on the blockchain’, 2022, [accessed 28 July 2022], https://blog.mollywhite.net/abuse-and-harassment-on-the-blockchain/.

47 BBC, ‘Metaverse app allows kids into virtual strip clubs’, 2022, [accessed 3 September 2022], https://www.bbc.com/news/technology-60415317

48 BBC, ‘Roblox: The children’s game with a sex problem’, 2022, [accessed 3 September 2022], https://www.bbc.com/news/technology-60314572

Different spaces in the metaverse need moderating for different behaviours.

A metaverse may present the perfect place for online sexual grooming. It may provide child sex offenders with opportunities to engage with children (i.e. through games) and deepen their interaction with children and/or escalate behaviour without having to leave this environment. Currently, offenders have to persuade children in an online game, social media or chatroom to give out personal details – in the metaverse offenders may be able to carry out the entire grooming process without such barriers. It will be very difficult for children to distinguish adults from other children since it would be difficult to know, especially for children, who they are talking with. These circumstances will provide a dangerously enabling environment for grooming efforts and any other form of (sexual) exploitation of children.

Haptics and advances in tactile technologies open up a sensory dimension to user interactions. This presents another challenge in safeguarding children online. For example, could offenders be virtually brought into a child's room with the ability to actually physically sexually abuse them through the child's haptic devices - without the offenders even having to leave their homes?

A metaverse may allow users to produce CSAM as well. Even if children are not involved, law enforcement may still need to respond. With the visual presentations of avatars becoming more realistic and the use of haptics adding a physical dimension to these experiences, this may be reason for concern. It will be important to find appropriate regulation for these kinds of situations and measures for detection, removal and prevention.

Any attempt by the platforms to moderate content and behaviour in the metaverse will inevitably be imperfect, leaving children open to being targeted. Since everything that happens in the metaverse is virtual, it presents a challenge for policing. The experience is becoming ever more immersive and real, generating an increasingly real impact, but it may not qualify for the legal terms of (sexual) abuse since the legislation stipulates for physical acts. Moreover, technical means to investigate on such platforms as well as adequate preventative measures lack for law enforcement to be able to act on these issues. Therefore, law enforcement will need civil society and policy makers to have discussions on what deviant behaviour in virtual worlds is to be considered criminal, and how they can get the legal and technical tools to act on this.

Another form of abuse originates from the ability to earn money through these platforms. Children may engage in projects to create mini-games or experiences for these platforms. These projects may lead to pressure on the children to work more, while the money generated through the game may not end up evenly distributed to all

contributors. This leads to abuse and exploitation of the children, in other words child labour.[49]

Terrorism

Terrorists will always try to exploit new technological options to facilitate their activities[50]; in the case of the metaverse, this may lead to new opportunities for terrorist organisations, primarily for propaganda, recruitment and training.

With more immersive technology and related generated data at their disposal, it will become easier for terrorists to select and target vulnerable people and tailor their messages to their biases. That will enable them to more effectively target their propaganda and recruit people.

With virtual environments becoming more realistic, this may provide an increasingly useful environment for training, both in generally available applications and in specifically (re-)created environments and scenarios. As an increasingly accurate and complete digital twin of reality becomes available, this may provide real-time information on planned targets. At some point, this may even allow for military reconnaissance and planning to be carried out within the metaverse.

On the other hand, the metaverse may allow users to create a virtual world as they envision the world should be, enabling them to create a virtual Caliphate or white supremacist state for example. Members of such places could live their virtual lives according to rules that may contradict fundamental laws and values of the society they live in in the physical world. For context, Nazi gas chambers have already been reported in Roblox.[51]

These virtual worlds may even allow them to impose their extremist rules on anyone entering their 'state'. This would create a truly parallel world for these people to live in and act out scenarios that undermine general acceptance of rule of law. Moreover, such spaces would provide a perfect environment for recruiting for terrorist activities in other virtual worlds - and even the physical world.

49 The Guardian, 'The trouble with Roblox, the video game empire built on child labour', 2022, [accessed 9 August 2022], https://www.theguardian.com/games/2022/jan/09/the-trouble-with-roblox-the-video-game-empire-built-on-child-labour.

50 Nextgov, 'Violent extremists could find the metaverse a useful recruiting and organizing tool – and a target-rich environment.', [accessed 24 August 2022], https://www.nextgov.com/ideas/2022/01/metaverse-offers-future-full-potential-terrorists-and-extremists-too/360494/.

51 The Algemeiner, 'Children's Gaming Platform Removes 'Disturbing' Nazi Concentration Camp 'Experience' With Gas Chambers', 2022, [accessed 31 August 2022], https://www.algemeiner.com/2022/02/21/childrens-gaming-platform-removes-disturbing-nazi-concentration-camp-experience-with-gas-chambers/.

Mis- and disinformation

The current Web2.0 has given rise to the emergence of unprecedented precision in the capabilities to target specific demographics to influence their behaviour, whether it is for commercial or political gain.[52] The vastly increased amount of data the new devices can glean from users' immediate environment and from the users themselves will have the potential to have a far greater influence on people's behaviour. Since this may destabilise the communities law enforcement is tasked to protect and the influence may be used by criminals to target their victims too, Law enforcement should be mindful of this.

On the old internet, the ability to gather vast amounts of data about individual preferences and behaviour by gathering data available on social media and following what people do online created a digital trail. This trail could be used to manipulate, identify and classify people online. The more immersive interactions enabled by metaverse-related technologies will create a far bigger digital trail. Unprecedented amounts of data will be gathered that allows for far greater insights and predictive power of behaviour, and may allow for the identification of individuals based on the uniqueness of these interactions.

Insights into people's preferences and behaviour allows not just for more accurate targeting of information, it may also allow for tailoring of content according to these insights. Both by employing these insights to maximise the chances the intended target is receptive to a specific message, and by utilising the immersion of the experience, the power exerted over user behaviour could increase.

At the same time, misinformation may become impossible to take down as its proliferation is increasingly decentralised with Web3 technology becoming more widely adopted.

Feasibility of monitoring/logging evidence

Policing the metaverse(s) will be a big challenge. A big responsibility will fall on the organisations that provide the platforms to monitor and moderate what happens on their platforms and to provide law enforcement with the tools to do their job on these platforms. As with current online activities, this will not be easy and the challenges there will be amplified and exacerbated with new issues to overcome.

The nature of metaverse(s) will make policing it more difficult, for reasons such as:

52 Bastick, Z., 'Would you notice if fake news changed your behavior? An experiment on the unconscious effects of disinformation', Computers in human behavior, Volume 116, March 2021, p. 106633, [accessed 22 August 2022], https://doi.org/10.1016/j.chb.2020.106633

- As the number of platforms and spaces is expected to proliferate, it will be impossible to police them all in an equivalent of patrolling the streets with the limited resources available.
- The challenges of monitoring what happens online will be greatly amplified for the metaverse. It will not just be a matter of moderating vastly more content, but also of behaviour, which is both ephemeral in nature and even more context-dependent than the content we are currently used to.
- Interactions in these worlds may become ephemeral as in the real world,[53] meaning there will be no traces left behind of your interactions. If this is the intended nature of such a world, it will become hard to gather evidence.
- Moreover, it may be hard to determine the 'reality' that was experienced by all parties involved.
- Lastly, with more of people's interactions moving to the metaverse the loss of location will increase. With increasing difficulties to establish the location of a user, the criminal infrastructure or access device used, law enforcement will face challenges in establishing which country has jurisdiction and which legal framework will apply.[54]

And what if unacceptable behaviour has been detected and it needs to be punished; how can crimes be effectively punished in the metaverse? Suspending an account may just lead to someone opening another, while finding a perpetrator in the physical world and enforcing the law where they live may be a big challenge as well. This is not a new challenge, but one that may be further exacerbated if a platform is based on decentralised and anonymising technology.

Impact in the physical world

With XR, the metaverse may affect the user's actions in the physical world. This is true through the presentation of a virtual reality, either as an overlay or as a fully immersive image, while in the metaverse. Having users experience the world through their metaverse devices will open them to exploits based on the control of this virtual (layer of) reality.

An immersive XR experience provides an opportunity to influence a user in the physical world through the manipulation of the virtual environment. Users can be tricked into hitting objects and walls, or being moved to another physical location, through what is called a 'Human Joystick Attack'. A perhaps simpler way is to alter the boundaries of a user's virtual world through a 'Chaperone Attack'.

53 Nick Clegg, 'Making the metaverse: What it is, how it will be built, and why it matters', 2022, [accessed 24 August 2022], https://nickclegg.medium.com/making-the-metaverse-what-it-is-how-it-will-be-built-and-why-it-matters-3710f7570b04.

54 Europol and Eurojust, 'Common challenges in combating cybercrime', 2019, [accessed 6 September 2022], https://www.europol.europa.eu/publications-events/publications/common-challenges-in-combating-cybercrime.

A third attack type is the 'Overlay Attack', in which the attacker takes complete control over the user's virtual environment and provides their own overlay – the input which defines what users see and perceive in a virtual environment.[55] These kinds of vulnerabilities should firstly concern the companies developing XR devices. Once this kind of vulnerability gets exploited, it may involve law enforcement depending on the seriousness of the result.

If a lot of unwanted and criminal behaviour goes unregulated and perpetrators are not held to account, this may result in a toxic and violent environment. Underlying mental health issues may be further aggravated if one's reality is deliberately manipulated by mis- and disinformation campaigns seeking to condition and control people. It could even destabilise people to the extent that it makes them struggle to distinguish between what is real and what is not.

Would it be possible for someone draws a real gun in self-defence to an XR threat? Do we consider a person (fully) accountable for these actions in the same way without this blended reality? In addition, how can we assess how convincing such an experience is, and if it warrants diminished accountability for the resulting actions? Finally, how should police respond to someone who is a physical threat because he/she is under threat from XR realities? These questions may influence police work and what we expect from law enforcement in this future.

LE use of metaverse (and related technology)

Being present regardless of distance

Since the COVID-19 pandemic, remote working and teleconferencing software has become widely adopted. The metaverse could allow people to come together in the same virtual room to work. This would allow for a more in-person experience than with current remote working technology, despite team members still being geographically dispersed. With this, it may become feasible to more flexibly compose teams of people with the right expertise for the case at hand and to facilitate interregional and international cooperation.

The metaverse as a place where people meet and can therefore facilitate the contact with the citizens law enforcement is tasked with protecting as well. It will allow officers to be more readily approachable for people in more sparsely populated areas and digital natives that spend most of their time in a virtual world. Just patrolling in a virtual car driving around a metaverse will probably not work very well with potentially endless worlds, both for deterrence as well as for being approachable. It will likely at least require tools for officers to be easily found by people looking for them and platforms to thoroughly monitor and easily alert police in case of possible criminal activities.

55 Casey, P., Baggili, I. and Yarramreddy, A., 'Immersive virtual reality attacks and the human joystick.', IEEE Transactions on Dependable and Secure Computing, , 2019, 18(2), pp.550-562.

Practically people in the metaverse may just want one 'Help!' function without looking for a representative of the police unit of their physical hometown. Efficient and effective metaverse policing may require international cooperation to effectively do this, and this may extend to between the moderators of the platform and the police. For the latter, a clear division of work is required, regardless of the level of cooperation.

Training

VR and XR allows one to experience a situation or environment independent of space and time. This opens up new possibilities for training. It allows for the training of rare situations and safe experience of situations that may be physically dangerous when experienced in the physical world.

Virtual crime scene

Where this technology can be taken a step further than just a picture of a crime scene is by adding real-world data and simulation to fully render a crime scene, including objects and actors in high definition and using machine learning to simulate the occurrence in full detail. Because of the accessibility of the metaverse, potentially both judge and jury could log in and review the simulation in their own time. The immersive aspect offered, similar to a VR scene, would allow them to view the crime from any perspective. The metaverse could allow for the creation of an immersive environment for the criminal justice system to allow us to:

- understand criminal acts from multiple perspectives;
- view crime scenes fully rendered and in high resolution using photogrammetry;
- overlay real-world data using digital twin information to simulate the crime taking place.[56]

Virtual experience can also be used to train officers for many different tasks by immersing them in any situation. An example is training for interactions with persons with severe mental illness. This training helps them recognise the issue and learn how to try to de-escalate the situation.[57]

The Netherlands Police created a virtual reality tool to combat ethnic profiling. This tool places the officer in a simulated situation in which they can take action based on what they experience. After completing these scenarios, they receive feedback and

56 Metapunk, 'Using the Metaverse to Simulate Crime Scenes', 2021, [accessed 21 July 2022], https://www.metapunk.co.uk/metablog/7-2021-using-the-metaverse-to-simulate-crime-scenes.

57 Force Science, 'Virtual Reality: The Next Step in Police Training', 2019, [accessed 30 July 2022], https://www.forcescience.com/2019/05/virtual-reality-the-next-step-in-police-training/.

discuss their performance to learn of potential biases in day-to-day police activities.[58]

A next step in this evolution could be the virtual presence of officers at a crime scene to help with the investigation. This would take it another step towards a metaverse application.

Alternative punishments/interventions

A unique property of an immersive experience is that it allows you to experience a reality you could not otherwise. This can be exploited to help create awareness of and empathy for the victim's position with offenders. Virtual reality experiences are being used to have people experience something from another perspective. This is, for instance, being used to have domestic violence offenders experience the victim's perspective in order to create empathy to reduce the chance they will commit to violence again.[59]

What to do and what is being done?

Build your online presence and experience the metaverse

Many countries have been investing in online policing, such as Estonia, Denmark, Norway, and Sweden. This is an important step to build valuable experience with virtual presence. Being present online makes police officers more approachable to people in remote locations and to people who spend most of their time online. With the great variety of available online platforms, it is important to gather experience on a few selected major platforms and build on the experience and tools acquired during this work.

Norway is a great example as it has started establishing its online presence in 2015 and now has 'Nettpatrulje' or internet patrols in every district. They are present on several different social media, gaming and streaming platforms with 509 000 followers for @ politivest on TikTok. A recent start on reddit's community r/norge saw 200 comments in the first hour and 200 000 views over the first weekend. This illustrates their advances with online policing. Moreover, Norway has been actively sharing their knowledge with other law enforcement agencies in Europe.[60]

France showed another example when it launched an initiative to establish a presence on Fortnite to be available for children suffering from abuse to share their stories.[61] Reaching out like

58 Het Laatste Nieuws, 'Antwerpse politie gebruikt voortaan virtual reality om etnisch profileren tegen te gaan: "Het scenario verandert naargelang de keuzes die ze maken in de simulatie."', 2021, [accessed 1 August 2022], https://www.hln.be/antwerpen/antwerpse-politie-gebruikt-voortaan-virtual-reality-om-etnisch-profileren-tegen-te-gaan-het-scenario-verandert-naargelang-de-keuzes-die-ze-maken-in-de-simulatie~a04dc477/

59 'France trials virtual reality 'empathy machine' on domestic violence offenders', 2021, [accessed 21 July 2022], https://www.rfi.fr/en/france/20210925-france-trials-virtual-reality-empathy-machine-on-domestic-violence-offenders-reverto.

60 Politiet, 'Police online patrols', [accessed 23 June 2022], https://www.politiet.no/en/rad/trygg-nettbruk/police-online-patrol/.

61 Gadgets 360, 'New Fortnite Mission: Reaching Out to Abused Children', 2020, [accessed

this can build valuable experience for how to establish an online presence and what different goals you can achieve when doing this.

While retaining an online presence on social media will still be very different from policing metaverses, it is an important first experience. This first step from the street into the online world will provide insights into how to be approachable and gain trust on online platforms. Moving to gaming platforms may add an extra dimension that yields more insights into policing open-ended and immersive worlds. These experiences are important to be able to understand and discuss what happens and could happen on these platforms. This is essential knowledge as law enforcement prepares to serve citizens in the metaverse and to formulate law enforcement's needs in conversations with the platforms.

Since online platforms are inherently global in nature, it is most effective to build a network of law enforcement experts on this subject. This will help facilitate the exchange of experience and tools, enabling law enforcement to formulate their requirements for operating in the metaverse more concisely. Making this a concerted effort will provide a stronger position and make compliance easier for platforms.

Recently Denmark, Norway and Sweden have taken the initiative with Europol to create a law enforcement working group on online policing. Law enforcement agencies throughout Europe will come together to share their experience and tools and make sense of (the development of) online policing together.

Start the conversation

With so much unknown about what the metaverse of the future will really be like, this may in fact be the perfect opportunity to start the discussion on law enforcement in the metaverse and how we think these platforms should work. This will allow us to discuss the possibilities offered by the platforms and figure out the best situation instead of just reacting after the fact.

What responsibility can metaverse providers and creators be expected to take for what happens on their platforms, and how can people best be served by their police forces in the metaverse? It will be essential to have civil society discuss what should be considered unacceptable behaviour and crimes in the metaverse.

Currently legislation is already lacking for present-day cybercrime and online interactions. With new types of experiences and possibilities in the metaverse, legislation will be found even more inadequate for the metaverse. Therefore, it will be important to raise awareness with our legislators of these issues and the tools

on 20 September 2022], https://gadgets360.com/games/features/new-fortnite-mission-reaching-out-to-abused-children-2247527.

law enforcement will need to fulfil their duties in these new virtual worlds.

Monitor and experience the metaverse and related technologies: know what is happening and what you are talking about

New technology, such as the internet when it first emerged, has been largely ignored by law enforcement organisations in the past, despite individual officers experiencing them in their private lives.

Legislating for new technology is often compared to driving a car only using the rear view mirror. It is often done in retrospect, and by that time new dangers are ahead of you, it is too late.
To anticipate what dangers may exist in the future is therefore vital is legislative bodies are to have any chance of getting to grips with potential problems.

Law enforcement needs to build experience in the metaverse and should find a way to make use of these private experiences, as they provide invaluable insight to make sense of what is happening and accurately assess new developments. We recommend law enforcement to monitor the development of the metaverse and to start building experience with online policing and early iterations of the metaverse. Doing this officially will help organisations stay informed on the subject and enable them to assess developments accurately, answering threats as they emerge.

It is essential for law enforcement to be accurately informed to meaningfully engage with companies, civil society and lawmakers. This will not only increase the chances of a serious discussion and for law enforcements concerns being heard, it may also help generate understanding of what police can achieve and perhaps even build some trust in our capabilities to do what we can do in the metaverse - if we can show we are well-informed of what we talk about.

Engage with companies creating it

In the early stages of development of any product, the foundations will be laid for the system based on the requirements known to the developers at the time. Retrofitting a system to new requirements will be a lot harder than including these in the beginning. Therefore, it is essential for civil society and law enforcement to share demands we place on these platforms early on in the adoption of the metaverse. Being in active conversation with the main actors developing the metaverse platforms is therefore essential, as it allows both sides to get a better understanding to help make the platform a safe place and adapt legislation and law enforcement to the challenge.

It might be interesting to find out how people want to contact the moderators of a platform or the police. If this means there

should be a way to immediately contact the relevant authority, this would be a feature that should be discussed. Perhaps there should be an API standard for law enforcement to connect to all platforms for such policing needs. These kinds of demands should be made known as early as possible in the development of the platform. Perhaps it could even be part of industry standards for interoperability of metaverses like the metaverse standards forum.[62]

62 Metaverse Standards Forum, 'Leading Standards Organizations and Companies Unite to Drive Open Metaverse Interoperability', 2022, [accessed 3 August 2022], https://metaverse-standards.org/news/press-releases/leading-standards-organizations-and-companies-unite-to-drive-open-metaverse-interoperability/.

Conclusion

The metaverse is still a long way from the visions that are presented to us by those developing and investing in metaverses and related technology. There is no way of knowing yet how these developments will exactly turn out, but the technology is rapidly evolving. Each evolutionary step can be expected to have a real impact on society and law enforcement. The history of the internet and other mainstream technologies has taught us that many unforeseen applications will likely emerge. Unanticipated side effects of a technology can ultimately have the biggest influence. Whatever may come of it, there is a need for law enforcement to get out there and experience the technology to stay abreast of these developments. Having an understanding of what is being developed will be essential for engaging all relevant actors and building a picture of the needs and responsibilities of law enforcement in the metaverse.

Undoubtedly, it is wise to start building experience with establishing a presence online in virtual worlds and using the technology that is already available. Online policing is a good way to experience what it means to have an online presence and to commence establishing international cooperation. Meanwhile, the experience gained from investigations into areas such as blockchain and NFTs will yield valuable information, experience and skills for law enforcement organisations.

For law enforcement to be successful in their explorations, it will be essential to pay special attention to the dissemination of ongoing efforts with relevant technology and online and virtual environments. The experience should not stay with the team that is working on it, but has to reach further into the organisation to create an organisational awareness of the challenges and opportunities that lie ahead. Building an international network of law enforcement experts on the subject to exchange on these experiences will help build knowledge faster and more efficiently.

With this primer, the Observatory Function of the Europol Innovation Lab hopes to have contributed to raising awareness of and demystifying the metaverse. We will further contribute to the discussion when developments warrant another look. In the meanwhile, the Innovation Lab will continue to support European law enforcement agencies in setting up an online policing network to help build and exchange experience on the subject.

About the Europol Innovation Lab

Technology has a major impact on the nature of crime. Criminals quickly integrate new technologies into their modus operandi, or build brand-new business models around them. At the same time, emerging technologies create opportunities for law enforcement to counter these new criminal threats. Thanks to technological innovation, law enforcement authorities can now access an increased number of suitable tools to fight crime. When exploring these new tools, respect for fundamental rights must remain a key consideration.

In October 2019, the Ministers of the Justice and Home Affairs Council called for the creation of an Innovation Lab within Europol, which would develop a centralised capability for strategic foresight on disruptive technologies to inform EU policing strategies.

Strategic foresight and scenario methods offer a way to understand and prepare for the potential impact of new technologies on law enforcement. The Europol Innovation Lab's Observatory function monitors technological developments that are relevant for law enforcement and reports on the risks, threats and opportunities of these emerging technologies. To date, the Europol Innovation Lab has organised three strategic foresight activities with EU Member State law enforcement agencies and other experts.

www.europol.europa.eu