The Global Business Law Review

Volume 12 | Issue 1 Note

12-8-2023

Our Changing Reality: The Metaverse and the Importance of Privacy Regulations in the United States

Anushkay Raza
Cleveland State University College of Law, r.anushkay@cmlaw.csuohio.edu

OUR CHANGING REALITY: THE METAVERSE AND THE IMPORTANCE OF PRIVACY REGULATION IN THE UNITED STATES

ANUSHKAY RAZA*

ABSTRACT

THIS NOTE DISCUSSES THE LEGAL AND PRESSING DIGITAL CHALLENGES THAT ARISE IN CONNECTION WITH THE GROWING USE OF VIRTUAL REALITY, AND MORE SPECIFICALLY, THE METAVERSE. AS THIS DIGITAL REALM BECOMES MORE INTEGRATED INTO OUR DAILY LIVES, THE UNITED STATES SHOULD LOOK TOWARDS CREATING A FEDERAL PRIVACY LAW THAT PROTECTS FUNDAMENTAL INDIVIDUAL PRIVACY RIGHTS. THIS NOTE ARGUES THAT CONGRESS SHOULD EMULATE THE EUROPEAN UNION'S PRIVACY REGULATIONS, AND FURTHER, BALANCES THE POTENTIAL CONSEQUENCES AND BENEFITS OF ADAPTING EUROPEAN REGULATIONS WITHIN THE UNITED STATES. FINALLY, THIS NOTE PROVIDES DRAFTING CONSIDERATIONS FOR FUTURE LAWYERS WHO WILL NOT ONLY BE DEALING WITH THE RISE OF PRIVACY IMPLICATIONS WITHIN THE METAVERSE, BUT ALSO ARTIFICIAL INTELLIGENCE, AND FURTHER TECHNOLOGICAL ADVANCEMENTS.

* J.D. expected May 2024, Cleveland State University, Cleveland State University College of Law. Anushkay graduated Summa Cum Laude from McGill University in 2021. I would like to thank *The Global Business Law Review*, and my family and friends for their endless support and encouragement. Special thanks to Professor Christa Laser, and Frank Camardo for their valuable direction in writing this note, to Professor Brandon Stump for introducing me to legal writing, to Dorothy Swagler for her constant guidance, and to my partner Murtaza Abbas for his unlimited positivity and love.

I. Introduction

What do you think of when you hear the word "metaverse"? A few say gaming and evoke concepts of a virtual reality, but most others think of fiction, or a far away and distant version of what technology will be like in the future. The metaverse is no longer a distant future; it is here, and it is acquiring larger amounts of traction from bigger tech companies like Facebook and Microsoft. The implication of this reality is a dystopian nightmare, and if left unregulated can impact all our lives.

The metaverse is an immersive virtual reality world where users can interact using digital avatars.[1] Users can join the metaverse through a Virtual Reality headset, which will function as a gateway to the world.[2] With the headset, there are three-dimensional glasses and a speaker set included, so that the user can physically feel as if they are a part of this augmented reality.[3] As a result of the pandemic, there has been a shift to virtual reality in different areas of life due to the

[1] Congressional Research Service, *The Metaverse: Concepts and Issues for Congress*, CRS REPORT (Aug. 26 2022), https://sgp.fas.org/crs/misc/R47224.pdf.
[2] *Artificial Intelligence in the Metaverse: Bridging the Virtual and Real,* XR TODAY (2022), online at https://www.xrtoday.com/virtual-reality/artificial-intelligence-in-the-metaverse-bridging-the-virtual-and-real/.
[3] *Id.*

recent rise in people who want to, and are able to, work from home.[4] With the rise of this interest in virtual reality, and an interest in looking for new spaces in order to be able to work or learn without leaving the house, many industries within healthcare, education, commerce, and social media, are already shifting towards virtual reality.[5] For example, a real estate company named the Metaverse Group just bought a parcel of land on a virtual real estate platform known as Decentraland for 2.45 Million US dollars.[6] This allows the company to hold showings online, find new clients from all over the world, and expand their business online and in person. The developments around the metaverse will bring forward many new and important legal implications surrounding privacy, specifically by reproducing and enlarging privacy, criminal, and surveillance issues that already exist around current corporations and online platforms.[7] As the world shifts to a more online realm, the threat of user's data being compromised and closely followed, become much more vital.[8] While we do not completely live in the metaverse yet, it is not far before a lot of our technology will be shifted towards it, and a lot of companies, and people will be collaborating on it.[9] It is unsettling to think about society living in a world fully dominated by loosely regulated technology companies, and individuals that have access to everyone's information. The solution is quite simple, and one that is already giving way in many other countries such as those in the European Union: the United States needs laws that will protect users when the metaverse becomes a substantial and real part of our everyday lives.

---

[4] *Id.*
[5] *Id.*
[6] Manas Sen Gupta, *The Metaverse Explained: What It Is And How It Works*, AUGUSTMAN (Dec. 6, 2021), https://www.augustman.com/sg/gear/tech/what-is-metaverse-and-how-does-it-work/.
[7] Nitin Kumar, *Six Unaddressed Legal Concerns for the Metaverse*, FORBES (Feb. 17, 2022), https://www.forbes.com/sites/forbestechcouncil/2022/02/17/six-unaddressed-legal-concerns-for-the-metaverse/?sh=7d383adb7a94.
[8] Cameron F. Kerry et al., *Bridging the Gaps: A Path Forward to Federal Privacy Legislation*, BROOKINGS INST. J. (June 2020).
[9] *Id.*

A pressing digital challenge ahead of us will be keeping up with the metaverse, and to do so, the United States must update its current laws on privacy. The lack of regulation should be regulated by Congress, because the metaverse opens a large window where consumers can have their privacy and data rights violated by individuals or corporations. This paper argues that Congress should enact a legal framework to protect fundamental privacy rights when it comes to the metaverse. Specifically, Congress should look to the European Union's General Data Protection Regulation, and their Digital Services Act to emulate three important rules: (1) companies and individuals should be controlled from selling individual's data without their consent; (2) there must be an enforcement mechanism that monitors companies and individuals; and (3) the data protection should include forms of regulation for biometric data, targeted advertisement, and criminal behavior such as abuse, fraud, and identify theft. Going forward, Part II of this Article provides a background of: (a) data privacy and why it is important; (b) the metaverse and the future expansion of it in businesses and everyday lives to illustrate the very real and upcoming problem with the metaverse's expansion; (c) the potential criminal implications that could arise within the metaverse; (d) any existing privacy legislation in the United States; and (e) the existing privacy and metaverse regulation in the European Union. Finally, Part III of this paper illustrates that the European Union's framework is possible to adapt within the United States because it would be protected by the Constitution through the Commerce and Supremacy clause, and it would not be opposed by businesses, who could instead actually benefit from the framework being implemented.

II. Background: A Look into the Metaverse and Data Privacy

A. What is Data Privacy and Why is it Important?

Data privacy is the right to control one's individual personal identifiable information (PII).[10] A PII is "any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means."[11] What constitutes a PII can vary, however generally some examples include: social security numbers, bank account numbers, full names, biometric records, place of birth, date of birth, and private information that could reasonably allow a regular person to be able to discern an individual's identity.[12] The idea of privacy, being alone, free from the surveillance of others, and having the choice of what information to give to others, encompasses data privacy.[13] To have privacy, there must be data privacy. In other words, to have privacy, an individual must be able to control the accumulation, and circulation of their individual personal information.[14] Without the ability to control one's own privacy, effectively everything about them can become public knowledge for the use of public consumption, sometimes to their own detriment.[15]

While privacy is something most people consider incredibly important to them, it has been largely left unregulated within the United States. With the rise of the metaverse, and lack of

[10] *What is Data Privacy?*, STORAGE NETWORKING INDUS. ASS'N (Feb. 22, 2023), https://www.snia.org/education/what-is-data-privacy.
[11] *Guidance on the Protection of Personal Identifiable Information*, U.S. DEP'T OF LABOR (Feb. 22, 2023), https://www.dol.gov/general/ppii#:~:text=Personal%20Identifiable%20Information%20(PII)%20is,either%20direct%20or%20indirect%20means.
[12] *Id.*
[13] *What is Online Privacy? And Why is it Important?*, BITDEFENDER (Feb. 22, 2023), https://www.bitdefender.com/cyberpedia/what-is-online-privacy/.
[14] *Id.*
[15] *Id.*

regulation in this realm, many individuals will find that the privacy they desire will cease to exist.

B. What is the Metaverse?

The metaverse is an informal term used to describe a network of immersive three-dimensional virtual worlds where users can play, socialize, interact, create, and explore through their digital avatars.[16] Activities in the metaverse are carried out through manipulating technologies like augmented reality (AR)[17], virtual reality (VR)[18], and blockchain[19], and they are used to create a virtual reality which mimics our physical world.[20] This virtual reality is designed to become a digital alternative to the physical world. In the metaverse, digital currency

[16] Ramandeep Singh, *User protection in the metaverse*, TATA CONSULTANCY SERVICES (2021), https://www.tcs.com/what-we-do/research/white-paper/user-privacy-protection-metaverse-experience.
[17] *Augmented Reality*, MERRIAM- WEBSTERS DICTIONARY, https://www.merriam-webster.com/dictionary/augmented%20reality (last visited Nov. 21, 2022) ("An enhanced version of reality created by the use of technology to overlay digital information on an image of something being viewed through a device [such as a smartphone camera]").
[18] *Virtual Reality*, BRITANNICA, https://www.britannica.com/technology/virtual-reality (last visited Sept. 8 2022) ("the use of computer modeling and simulation that enables a person to interact with an artificial three-dimension (3-D) visual or other sensory environment. VR applications immerse the user in a computer-generated environment that stimulates reality through the use of interactive devices, which send and receive information and are worn as goggles, headsets, gloves, or body suits.").
[19] *Blockchain*, OXFORD LEARNERS DICTIONARIES, https://www.oxfordlearnersdictionaries.com/us/definition/english/blockchain (last visited Nov. 1, 2023) ("A system in which a record of payments made in cryptocurrency is maintained across several computers that are linked.").
[20] Lik-Hang Lee, *All One Needs to Know about Metaverse: A Complete Survey on Technological Singularity, Virtual Ecosystem, and Research Agenda*, RESEARCHGATE (Oct. 2021), https://www.researchgate.net/publication/355172308_All_One_Needs_to_Know_about_Metaverse_A_Complete_Survey_on_Technological_Singularity_Virtual_Ecosystem_and_Research_Agenda.

is used to buy clothes and items, and that currency is leveraged through cryptocurrencies[21], and non-fungible tokens[22].

The concept of the metaverse, while seemingly recent, has not been a new idea. The first description of the metaverse was given in the novel *Snow Crash* by Neal Stephenson, who painted the metaverse as a dystopian next generation virtual reality-based internet. A few years later, the term was popularized by director Steven Spielberg, in his film adaptation of *Ready Player One* by Ernest Cline.[23] In this film, users elude the problems that are facing Earth by disappearing into a virtual world called the Oasis.[24] The dominant concern that both artists allude to is the issue of privacy violations on a much larger scale; in which every user interacting on these technologies is being surveilled, and there is an increase in virtual crimes that have been left unregulated.[25]

In one of the most influential essays on the Metaverse, the author Matthew Ball establishes seven main characteristics of the metaverse: (1) it will go on indefinitely; (2) it will be synchronous and live; (3); there will be no limit on the number of users; (4) there will be a fully functioning economy in which businesses and individuals will be able to work, and earn;

---

[21] *Cryptocurrency*, OXFORD LEARNERS DICTIONARIES, https://www.oxfordlearnersdictionaries.com/us/definition/english/cryptocurrency#:~:text=%2F%CB%88kr%C9%AApt%C9%99%CA%8Ak%C9%9C%CB%90r%C9%99nsi%2F,need%20for%20a%20central%20bank (last visited Nov. 1, 2023) ("any system of electronic money, used for buying and selling online and without the need for a central bank").

[22] Rakesh Sharma*, Non-Fungible Token (NFT): What It Means and How It Works*, INVESTOPEDIA (Jun. 22, 2022) https://www.investopedia.com/non-fungible-tokens-nft-5115211#:~:text=NFTs%20(non%2Dfungible%20tokens),reducing%20the%20probability%20of%20fraud (providing that NFTS are unique crypto tokens that exist on blockchain technology, and represent real world tangible assets that make buying, selling and trading them online more efficient).

[23] Charlie Fink, *The Reality of Virtual Reality In 'Ready Player One'*, FORBES (Oct. 23, 2017), https://www.forbes.com/sites/charliefink/2017/10/23/the-reality-of-virtual-reality-in-ready-player-one/?sh=5137e79c20d0.

[24] Linda Tucci, *What is the Metaverse? An Explanation and in-depth guide*, TECH TARGET (Nov. 18, 2022), https://www.techtarget.com/whatis/feature/The-metaverse-explained-Everything-you-need-to-know.

[25] *Id.*

(5) there will be private and public experiences; (6) there will be an increase in the forms of technologies supporting the metaverse; and (7) it will be populated by content and experiences created by a variety of contributors.[26] Ultimately, Matthew Ball described the metaverse as another universe, in which people can create the lives that they want.[27] To this day, it has been a very accurate description of the characteristics of the metaverse, and can be used to illustrate the involved and intense nature of it.[28]

C. Our Society's Move Towards the Metaverse: How it Has Grown

The largest corporation to enter a virtual space has been Facebook in 2021, when Mark Zuckerberg introduced Meta to take the first step towards the creation of this dystopian reality. In doing so, Zuckerberg illustrated the ability for the metaverse to interconnect with social media, especially mainstream applications such as Facebook, and Instagram.[29] When introducing Meta to the world, Zuckerberg proposed a virtual space in which everything people do in the real world is replicated.[30] Similarly, Microsoft also created their own version of the Metaverse: MESH, in which one of their innovations included the concept of 'holoportation', in which users will be able to project their holographic selves as avatars to others.[31]

This interest did not end with tech giants; there is a growing interest in the metaverse spanning a large variety of demographics, from children to professionals. Several aspects of the

[26] Matthew Ball, *The Metaverse: What It Is, Where to Find it, and Who Will Built It*, MATTHEWBALL (Jan. 13, 2020), https://www.matthewball.vc/all/themetaverse.
[27] *Id.*
[28] *Id.*

[29] *Introducing Meta: A Social Technology Company,* META (Oct. 28, 2021) https://about.fb.com/news/2021/10/facebook-company-is-now-meta/.
[30] *Id.*
[31] Gupta, *supra* note 6.

metaverse are already being used, including in commerce, entertainment, and education.[32] First, within commerce, major companies have already moved towards accepting cryptocurrencies as forms of payment for goods and services.[33] Further, companies are showing a move towards developing reality occupational training models, and marketing and advertising their own products and services within the metaverse through virtual events, storefronts, and digital collectibles.[34] An example of a company that has taken this to the next level is Nike, that has created a Metaverse space called Nikeland; allowing fans to meet, socialize, take part in promotions, and buy their avatars Nike shoes with cryptocurrency.[35] Video games have also already seen large success in the metaverse. For example, Roblox Metaverse, which has a huge user base, gained much attraction and growth during the pandemic because it allowed video game users to create their own virtual worlds within the metaverse to attend concerts, emulate themselves within the games, and join in on brand content collaborations.[36] This showcases that, through companies such as Roblox within the Metaverse, the idea of how entertainment can be provided has expanded. For example, many artists are having virtual concerts within the metaverse, where they are provided with a bigger platform to interact with their fans. [37] Some

[32] Vladislav Boutenko, *The Metaverse Will Enhance-Not Replace-Companies' Physical Locations*, HARV. BUS. REV. (Aug. 18, 2021)
[33] *Id.*
[34] *Id.*
[35] Bernard Marr, *The Amazing Ways Nike Is Using The Metaverse, Web3 And NFTs*, FORBES (Jun. 1, 2022), https://www.forbes.com/sites/bernardmarr/2022/06/01/the-amazing-ways-nike-is-using-the-metaverse-web3-and-nfts/?sh=d91eaf356e94
[36] Akhil Taneja, *Everything You Need To Know About Roblox Metaverse*, CASHIFY TECH BYTE (Oct.21, 2022), https://www.cashify.in/roblox-metaverse-things-you-need-to-know.
[37] Emma Chui, *Sound On in the Metaverse: Why It's Just the Beginning for Virtual Concerts*, WUNDERMAN THOMPSON INTELLIGENCE MUSE (Sept, 19. 2022) https://musebycl.io/music/sound-metaverse-why-its-just-beginning-virtual-concerts#:~:text=Caught%20in%20the%20metaverse.,more%20have%20announced%20upcoming%20shows.

celebrities that have already began doing virtual concerts include Dua Lipa, Lil Nas X, and the Foo Fighters.[38]

Aside from entertainment, there has been an initiative to migrate education towards a more virtual setting. This sentiment arose during the pandemic, when society saw a rise in interactive distance learning and education remotely.[39] These virtual classrooms are the beginning of the expansion of educational experience- not just in primary school, but also in higher learning. One example of this is in the healthcare industry, where many are looking to transform the industry by allowing health practitioners and residents to practice immersive surgical experience and interact with patients through the metaverse.[40]

All of this enhanced participation in the metaverse will include the involvement of the collection of unprecedented amounts of personal data, which reveal many possibilities for monetization and profit.[41] Users who participate in the Metaverse will be logged in for longer periods of times, which means that their behavior will continuously be monitored, and corporations will be able to gather data on each user's physiological responses, their brainwave patterns, and their intimate thought processes and behaviors.[42] All of these responses are what create an individual's unique biometric data, that is used to verify one's identity.[43] The ultimate implication of this is that a user's biometric data will be continuously monitored and gathered in

---

[38] *Id.*
[39] Ramandeep Singh, *User Privacy Protection in the Emerging World of Metaverse*, TATA CONSULTANCY SERVICES (2022), https://www.tcs.com/content/dam/tcs/pdf/discover-tcs/Research-and-Innovation/user-privacy-protection-metaverse-experience.pdf.
[40] *Id.*
[41] *The Metaverse: The evolution of a universal digital platform,* NORTON ROSE FULBRIGHT (Jul. 2021), https://www.nortonrosefulbright.com/fr-fr/knowledge/publications/5cd471a1/the-metaverse-the-evolution-of-a-universal-digital-platform
[42] *Id.*
[43] Alison Johansen, *Biometrics and biometric data: What is it and is it secure?,* NORTON (Feb. 8, 2019), https://us.norton.com/blog/iot/biometrics-how-do-they-work-are-they-safe# (illustrating that physiological traits and behavioral characteristics are used to create an individual's biometric data, which can be used to identify a person).

the background while they innocently participate in the metaverse.[44] The immersive technology functions in the metaverse will also further reveal details about user's likes, dislikes, and preference, and will further the possibilities of targeted advertising[45].[46] These empowers companies to have access to information that will "be akin to reading the user's mind."[47] With this high-level move towards the metaverse, there will be many individuals and companies sharing their information and their data. Without a legal privacy framework regulating this new area of the world, the move will be fraught with privacy challenges for users relating to consent and control, over the storage and high-level consumption of their information and personal data on company or individual databases, which can also then be used and/or stolen to engage in criminal activities online.

D. The Increase in Criminal Activity Within the Metaverse

In the metaverse, users can, and most likely will, recreate crimes that occur in the real world.[48] A form of crime that is likely to be replicated within the metaverse is cybercrime. Cybercrimes are defined as "acts committed through information and communication technologies that violate the law of the physical world."[49] Examples of some cybercrimes that

[44] *Id.*
[45] *What is Targeted Advertising?*, THE NOW (Mar. 1, 2023), https://edu.gcfglobal.org/en/thenow/what-is-targeted-advertising/1/#, ("Targeted advertising is a form of online advertising that focuses on the specific traits, interests, and preferences of a consumer).
[46] *Id.*
[47] Aisling Ni Chulain, *'Reading your mind': How eyes, pupils and heart rate could be used to target ads in the metaverse*, EURO NEWS (Mar. 03, 2021), https://www.euronews.com/next/2021/12/03/reading-your-mind-how-eyes-pupils-and-heart-rate-could-be-used-to-target-ads-in-the-metave.
[48] Europol, *Policing in the metaverse: what law enforcement needs to know*, PUBLICATIONS OFFICE OF THE EUROPEAN UNION (2022), https://www.europol.europa.eu/cms/sites/default/files/documents/Policing%20in%20the%20metaverse%20-%20what%20law%20enforcement%20needs%20to%20know.pdf.
[49] Michael Aaron Dennis, *Cybercrime*, BRITANNICA (Feb.22, 2023), https://www.britannica.com/topic/cybercrime/Identity-theft-and-invasion-of-privacy.

are likely to appear within the metaverse, are (1) identity theft and/ or phishing, (2) financial money laundering or scams; (3) terrorism, and/ or (4) child exploitation.[50]

Identity theft occurs when someone steals your personal information to commit fraudulent activities under your name, such as applying for credit cards, filing taxes, spending money, or even using your identity to engage in further criminal activity.[51] The increase in technologies that enhances the realism of digital identities, makes it more convenient for criminals to facilitate the unauthorized use and exploitation of one's physical identity.[52] In the metaverse, this can be attributed to the unfiltered access to users' biometric data, and behavioral information. With the collection of individual behavior and preferences, criminals can have access to not just physical identification characteristics, but also interactions that users have, what users like or dislike, and even their mannerisms.[53] As companies gain the ability to access this information and use it for targeted advertising or monetization, criminals can also gain the ability to access this information for more sinister reasons. The continuous monitoring of individuals and collection of data within the metaverse, sharpens the ability for criminals to imitate user's characteristics and behaviors.[54] Criminals can also sell digital fingerprints, and user's private information (such as their birthdays, their physical and behavioral characteristics, their biometric data) to other criminals that can use this information to steal their identity within the real world.[55] Aside from individuals, brands are also in a vulnerable position within the

[50] *Id.*
[51] Ali Hussain, *What is Identity Theft? Definitions, Types, and Examples,* INVESTOPEDIA (Marguerita Cheg ed., Feb. 22, 2023) https://www.investopedia.com/terms/i/identitytheft.asp.
[52] Europol, *Policing in the metaverse: what law enforcement needs to know*, PUBLICATIONS OFFICE OF THE EUROPEAN UNION (2022), https://www.europol.europa.eu/cms/sites/default/files/documents/Policing%20in%20the%20metaverse%20-%20what%20law%20enforcement%20needs%20to%20know.pdf.
[53] *Id.*
[54] *Id.*
[55] *Id.*

metaverse, as criminals can impersonate brands, something that is commonly done when phishing.[56] In the metaverse, this could be done through criminals creating fake stores that appear real and convince other users to give personal information in exchange for whatever services or goods they are purporting to offer.[57]

The second crime that should be subject to regulation is financial money laundering[58], or financial scams that exist within the metaverse, specifically regarding NFTs and the mishandling of other people's assets. Money and value take on an important shape within the metaverse, and the use of digital currencies are going to be used to make payments so that users can buy items quickly and effortlessly.[59] Virtual businesses will want to sell virtual goods to avatars, and in order to do that, there has to be virtual money. This creates opportunities for more money to be spread across different countries, cities, and areas, without the regular policing that occurs in the real world.[60] Thus, without authorities monitoring these currencies and exchanges, it is likely that there will be a higher risk of money laundering and an increased facilitation of criminal money transfers.[61] The anonymous and deceptive nature of the metaverse will it make it difficult for regular law enforcement to monitor these crimes.

---

[56] *Phishing,* MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/phishing (last visited Feb. 22, 2023) (a way that a perpetrator can acquire sensitive personal data through a fraudulent solicitation, in which the perpetrator
pretends to be a legitimate business or reputable person).
[57] *Id.*
[58] *Money Laundering*, OXFORD LEARNER'S DICTIONARIES (2023), https://www.oxfordlearnersdictionaries.com/definition/english/money-laundering#:~:text=%2F%CB%88m%CA%8Cni%20l%C9%94%CB%90nd%C9%99r%C9%AA%C5%8B%2F,%2F%CB%88m%CA%8Cni%20l%C9%94%CB%90nd%C9%99r%C9%AA%C5%8B%2F,where%20the%20mon, ("the crime of moving money that has been obtained illegally into foreign bank accounts or legal businesses so that it is difficult for people to know where the money came from").
[59] *See Metaverse and Money*, CITI GPS (Mar. 30, 2022), https://icg.citi.com/icghome/what-we-think/citigps/insights/metaverse-and-money_20220330.
[60] *Id.*
[61] *Id.*

The third crime that is likely to be an issue within the metaverse, is the increase in potential for terrorism; specifically, the increase in opportunities for propaganda, recruitment, and training.[62] With the access to unfiltered data on the metaverse, terrorists will find it easier to target and find vulnerable people, who are easily susceptible to their propaganda. Moreover, their ability to communicate to each other without surveillance will pose as a benefit to terrorist organizations.[63] Another big risk lies in their heightened chance to train recruits as well; with virtual environments becoming more realistic, terrorist organizations can create spaces that will allow them to carry out scenarios and teach their recruits their laws, and values; essentially, creating a virtual society for them to enhance their beliefs.[64] While it seems farfetched, a real life example of this is the existence of Nazi gas chambers were created by white supremacists in Roblox.[65]

Finally, another crime that has already been observed within virtual reality is child exploitation.[66] At the moment, there is no effective age limit in the metaverse.[67] Additionally, because of the lack of regulation in this area, there is no moderation of the content and behavior that children are encountering. The unregulated metaverse presents the perfect place for online sexual grooming and provides sex offenders and criminals with opportunities to engage with children through games, or through positing as their peers.[68] While criminals on the internet can

---

[62] Joel S. Elson, *The Metaverse Offers a Future Full of Potential—for Terrorists and Extremists, Too,* NEXTGOV (Jan. 7, 2022), https://www.nextgov.com/ideas/2022/01/metaverse-offers-future-full-potential-terrorists

[63] *See generally id* (explaining that the lack of oversight in the metaverse can allow for terrorist meetings in places that would be public in the real world).

[64] *Id.*

[65] Shiryn Ghermezian, *Children's Gaming Platform Removes 'Disturbing' Nazi Concentration Camp 'Experience' With Gas Chambers*, THE ALGEMEINER (Feb. 21, 2022, 2:06 PM), https://www.algemeiner.com/2022/02/21/childrens-gaming-platform-removes-disturbing-nazi-concentration-camp-experience-with-gas-chambers/.

[66] Europol, *Policing in the metaverse: what law enforcement needs to know*, PUBLICATIONS OFFI

[67] *Id.*

[68] *Id.*

interact with children in chat rooms and through social media apps, there are usually some limitations that exist, in the form of age restrictions, or secondary verification that the users are who they say they are. However, within the metaverse, offenders may be able to groom children without limitation, especially by pretending to be children, or by joining events, or games that children participate in.[69]

The aforementioned issues are of pressing concern especially because the metaverse does not have geographical borders and is open to practically every single person without filtered access. Thus, there is an urgent need to understand how to facilitate collaboration and crime investigation within the metaverse, and this can be done through the regulation of a privacy law and framework. Without some form of policing and regulation of the data that is being consumed and spread within the metaverse, criminals will a green light to steal information and data and create situations in which they are able to commit crimes against those who are most vulnerable in society.

E. Privacy Legislation in the United States

As of right now, there is no federal privacy framework that exists within the United States. However, there are 5 states: California, Colorado, Connecticut, Utah, and Virginia, that have created forms of their own privacy regulations.[70] The largest of them was California's, which was enacted on January 1, 2020, and is considered to be one of the most comprehensive

[69] *Id.*
[70] Theodore P. Augustinos and Alexander R. Cox, *U.S. State Privacy Laws in 2023: California, Connecticut, Utah and Virginia*, LOCKE LORD (Dec. 2022), https://www.ncsl.org/technology-and-communication/state-laws-related-to-digital-privacy#:~:text=Five%20states%E2%80%94California%2C%20Colorado%2C,of%20personal

privacy laws in the United States.[71] The remaining states that have privacy regulations (Colorado, Connecticut, Utah, and Virginia), have regulations that very closely resemble California's Act. Thus, due to the similarities, a look into California's regulations will give a thorough understanding of privacy laws within the United States. The California Consumer Privacy Act (CCPA) was enacted in 2018, to regulate businesses in California by allowing consumers to control the data that companies can collect about them. Consumers have the right to request businesses to disclose any personal information that the business has collected on them, the right to opt out of the sale of their personal information, and the right to delete the personal information that is collected from them.[72] Further, businesses are also required to give consumers notice regarding their privacy practices, and inform consumers of the time period that they intend to retain the individual's personal information.[73] The intent of the California Consumer Privacy Act was for the legislature to further ensure California resident's right to privacy, especially when it came to what businesses could or could not do with the consumers personal information.[74]

There are a few categories of companies that the California legislature intended to make sure were following the privacy regulations. The CCPA applies to companies that do business in the State of California[75], and that satisfy one or more of the following thresholds: (1) has annual

---

[71] *See generally* Rob Bonta, *California Consumer Privacy Act (CCPA)*, STATE OF CALIFORNIA DEPARTMENT OF JUSTICE, https://oag.ca.gov/privacy/ccpa#:~:text=The%20California%20Consumer%20Privacy%20Act

[72] CAL. CIV. CODE § 1798.100 (West 2023).

[73] *See* Lothar Determann, *New California Law Against Data Sharing: The California Consumer Privacy Act of 2018, Broad Data and Business Regulation, Applicable Worldwide*, 19 COMP. L. REV. INT'L., no. 4, 2018, at 117.

[74] *Id.*

[75] *See Doing Business in California*, CALIFORNIA CONSUMER PRIVACY ACT (CCPA) STATE OF CALIFORNIA FRANCHISE TAX BOARD, (Mar. 1, 2023) https://www.ftb.ca.gov/file/business/doing-business-in-

gross revenues in excess of twenty-five million dollars ($25,000,000); (2) alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices; and/or (3) derives 50 percent or more of its annual revenues from selling consumers' personal information.[76] The Act targets these companies because these are usually the businesses in which consumer privacy breaches occur. Thus, while it is clear that a few states have begun to recognize the importance of privacy over the last few years, there has been no explicit mention of the metaverse, or technology as powerful as the metaverse (such as virtual reality, or augmented reality), nor has there been a mention of increased cybercrimes that are likely to occur with the boosted use of these technologies.[77]

F. Privacy Legislation in the European Union: The General Data Protection Regulation (GDPR) & the Digital Services Act (DSA)

The General Data Protection Regulation (GDPR)[78] took effect throughout the European Union (EU) on May 25, 2018, and was said to have "opened a new chapter in the history of the Internet, and to have acted to protect a fundamental human right to privacy."[79] Through this

---

california.html#:~:text=We%20consider%20you%20to%20be,or%20commercially%20domiciled%20in%20California (highlighting that doing business is engaging in transactions with the purpose of gaining financially in California, and being organized or commercial domiciled in California).

[76] CAL. CIV. CODE § 1798.140 (West 2023).

[77] *See* Tatum Hunter, *Surveillance will follow us into 'the metaverse', and our bodies could be its new data source*, THE WASHINGTON POST (Jan. 13, 2022), https://www.washingtonpost.com/technology/2022/01/13/privacy-vr-metaverse

[78] *See generally* Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, 2009 O.J. (L 119) 1.

[79] Chris Mirasola, *Summary: The EU General Data Protection Regulation,* LAWFARE (Mar. 01, 2018), https://www.lawfareblog.com/summary-eu-general-data-protection-regulation#:~:text=The%20GDPR%20creates%20an%20EU,the%20entity%20holding

movement, the EU has taken a very significant role in influencing how the world thinks about data privacy.[80]

The GDPR's definition of personal data is "information relating to an identified or identifiable natural person", including not just general personal data (name, date of birth, or likes/dislikes), but also biometric and health data, as well as personalized data such as race, ethnicity, or religion.[81] The GDPR warrants several privacy rights to their citizens including notifications of personal data breaches, access to one's personal data, the freedom to require an entity to erase their personal data; and the capacity to move their personal data from one entity to another.[82] These privacy rights are to be enforced and applied against all corporate entities regardless of where the entity is located, if it is processing the personal data of EU citizens.[83] In summary, the goal of this Act is "to give citizens back control over their personal data."[84]

This regulation is forwarded through several means- (1) organizations that breach their consent requirements can be fined up to 4% of their global turnover; (2) under the GDPR, consent must always be clear and at times, explicit; (3) the corporations that have access to data subjects on a large scale must appoint a data protection officer who is in charge of GDPR compliance and works with the EU authorities; and (4) a data protection certification mechanism that tells companies when they are [or are not] in compliance with GDPR regulations.[85]

---

[80] *Id.*
[81] Regulation 2016/679, art. 4, 2009 O.J. (L 119) 1, 33.
[82] Regulation 2016/679, art. 13-17, 2009 O.J. (L 119) 1, 40.
[83] Regulation 2016/679, art. 47, 2009 O.J. (L 119) 1, 62.
[84] Natasha Lomas, *WTF is GDPR?*, TECHCRUCH (Jan. 20, 2018, 12:00 PM), https://techcrunch.com/2018/01/20/wtf-is-gdpr/; *see generally* EUROPEAN COMMISSION, https://commission.europa.eu/index_en (last visited Oct. 31, 2023)(providing full text and history of the regulation).
[85] Mirasola, *supra* note 79.

Alongside the GDPR, there exists the Digital Services Act (DSA), which was passed on July 5, 2022, by the European Commission in the EU.[86] The DSA's protection together with the GDPR has been labeled as the "gold standard" for content and data protection governance, and this standard will begin to apply in the EU from the 1st of January 2024.[87] The DSA is a targeted response to the growth in technological advancements, such as the metaverse, and is aimed to increase the transparency and safety for users in online, and particularly, virtual environments. The Digital Services Act brings significant outcomes that protects fundamental privacy rights online, specifically a strong ban on surveillance-based advertising and non-consensual data collection.[88] The primary importance of the DSA lies in the fact that it goes beyond just transparency and consent and creates a ban on advertising based on profiling and special categories of personal data (sexual orientation, political orientation, and or race).[89]

The final and most salient aspect of the DSA is that it allows government agencies within the European Union to uncover and remove potentially illegal or harmful content.[90] In other words, users in the metaverse, under the DSA's regulations will have a more difficult time promoting terrorism, or engaging in child harassment, etc.[91] Consequently, this element of the Act is focused on cybercrime, and preventing the illegal spread of information by criminals. The DSA also further imposes a ban on dark patterns[92], online advertising targeting minors, and the

[86] Commission Regulation 2022/2065, 2022 O.J.(277)
[87] *Id.*
[88] *Id.*
[89] *Id.*
[90] Dan Cooper, EU Adopts Digital Services Act, INSIDE PRIVACY (Oct. 10, 2022), https://www.insideprivacy.com/european-union-2/14067/#:~:text=On%20October%204%2C%202022%2C%20the,social%20networks%20and%20online%20marketplaces)
[91] *Id.*
[92] Jasmine McNealy, *What Are Dark Patterns?,* NEXTGOV (Aug. 3, 2021), https://www.nextgov.com/ideas/2021/08/what-are-dark-patterns-online-media-expert-explains/184244/ ("Dark patterns are design elements that deliberately obscure, mislead, coerce and/or deceive website visitors into making unintended and possibly harmful choices."

illegal accumulation of sensitive personal data without governance compliance.[93] The combination of these compliance measures will significantly hinder companies and individuals from unlawfully acquiring large amounts of personal data without consent. [94]

III. Possible Routes Towards Creating a Federal Privacy Law

As technologies continue to grow and advance, and the metaverse becomes more popular, the United States must explore different approaches to tackle the growing concerns of data privacy breaches and the implications of these breaches. One possible means of doing this is by emulating the EU's regulations in the GDPR and the DSA and use that to create legislation that provides a framework to protect users against data and privacy violations. This section of the paper discusses: (1) how individualized state laws on privacy do not provide much protection to consumers; (2) how Congress should look to the EU and their ideals of transparency and governance, which are embodied in three directives: (a) companies should be controlled from selling private data, (b) an enforcement mechanism should exist that protects and regulates how companies and individuals interact with consumer's data, and (c) data regulation should also include the protection of the individual's biometric data, and the individual from criminal activity stemming from data breaches; and (3) how the Constitution actually permits Congress to regulate privacy through the Commerce Clause and the Supremacy Clause, and how companies would, in turn, derive benefit from the enactment of this legislation.

[93] *Id.*
[94] *Id.*

A. The Problems with Individual State Laws on Privacy & The Benefits of the EU's Privacy Framework

While, California has the most comprehensive framework out of the five states that have a framework in the US, the remaining four states (Colorado, Connecticut, Utah, and Virginia) have similarly enacted privacy frameworks.[95] As a result of this, they all experience the same legal difficulties that inevitably make their state regulations less effective, and easier to bypass.[96] There are three major legal issues that arise with each of the individual state frameworks: (1) there is no explicit mention of the metaverse, virtual reality, or biometric data such as physiological movements, which means that there is not much protection being applied within the contours of the metaverse; and (2) there is no unified enforcement agency between the States; which means that there is no mechanism that uniformly enforces fines, punishments, and guidelines for individuals and companies. [97] Finally, the third biggest issue is that without a federal framework, there are still only five states that have privacy guidelines, which means that thousands of companies and individuals are going unregulated, and thousands of citizens are without any kind of protection either from unfair and targeted market practices or cybercrimes.[98] These issues need to be addressed within the federal privacy framework, and the EU's framework allows that to occur. Thus, when implementing the EU's framework, Congress will be providing a solution to these state level issues.

---

[95] Tony Romm*, Inside the lobbying war over California's landmark privacy law*, WASHINGTON POST (February 9, 2019), https://www.mercurynews.com/2019/02/09/californias-landmark-privacy-law-sparks-lobbying-war-that-couldwater-it-down/.
[96] Reed Smith, *Reed Smith Guide to the Metaverse,* 63, 64, eds., 2nd ed. 2002.
[97] Tony Glosson, *Data Privacy in Our Federalist System: Toward an Evaluative Framework for State Privacy Laws*, 67 FED. COMM. L.J. 409, 415 (2015). http://www.fclj.org/wp-content/uploads/2016/01/67.3.2-Glosson.pdf
[98] *Id.*

The DSA and the GDPR both share certain characteristics that establish data privacy regulations, safeguarding users from privacy infringements within the metaverse, and address concerns mentioned earlier.[99] By providing a federal framework for all countries to follow within the European Union, they are essentially solving these state [or country, in the case of the EU] level issues.[100] More precisely, the framework established by the EU concentrate on: (1) controlling companies and individuals from using or selling the individual's data without their consent; (2) creating enforcement mechanisms through an agency to monitor companies, and individuals within the network to enforce the specific guidelines set out within the Acts so that there is one unified agency that deals with data regulation; and (3) monitoring and including forms of advertising and criminal activity, based on personal data profiling, biometrics, and targeted advertisement, so as to protect the consumer within virtual reality and newer technological advancements such as the metaverse.[101]

Through the adoption of the above three rules, the European Union is calling attention to, and providing two important rights to the individual within the metaverse: the right to user transparency, which blends into the right to pursue civil or criminal actions against those who violate these rules.[102] First, the EU is illustrating the importance of the right to increased transparency amongst users and individuals, so that users can consent to and control their personal data, and control how it is being accessed or used. This inevitably ensures that users

[99] Matthias Artzt, *Territorial scope of the GDPR from a US perspective*, IAPP: THE PRIVACY ADVISOR (June 26, 2018), https://iapp.org/news/a/territorial-scope-of-the-gdpr-from-a-us-perspective/.
[100] Adam Satariano, G.D.P.R., *a New Privacy Law, Makes Europe World's Leading Tech Watchdog*, N.Y. TIMES (May 24, 2018), https://www.nytimes.com/2018/05/24/technology/europe-gdpr-privacy.html.
[101] E.U. General Data Protection Regulation (GDPR): Regulation (E.U.) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2009 O.J. (L 119) 1. (https://gdpr-info.eu/)
[102] Ben Wolford, *What is GDPR, the EU's new data protection law?*, GDPREU (2023), https://gdpr.eu/what-is-gdpr/.

train control of their data, preventing its inappropriate usage, and in turn, protecting them.[103] Second, by creating an enforcement mechanism to monitor companies, the EU is ultimately creating a private right to action for individuals that feel as if their privacy rights are being violated, or feel as if they have been the target of criminal activity.[104] A framework within the United States that encapsulates these qualities that the GDPR and the DSA offer will be the answer to the aforementioned challenges in the United States, and will provide a structure that safeguards thousands of individuals, especially those participating in the Metaverse. Ultimately, these are the features that should be implemented in a large-scale privacy framework within the United States.

B. How to Fit a Federal Privacy Framework Within the United States: The Constitutionality of Federal Privacy Laws

One major challenge to creating a national privacy law is whether Congress has the power to pass a law that creates privacy rights that have historically been reserved to the states. The 10th Amendment states that all rights that are not explicitly given to the federal government are reserved to the states.[105] Thus, since the right to regulate privacy is not explicitly written in the Constitution as a federal right, states have the power to regulate privacy. This problem can be resolved through the Commerce Clause, which allows the government to regulate activities or things related to or facilitating commerce (the buying and selling of goods) between states.[106] The Commerce Clause power stems from the Constitution, and is located in Article 1, Section 8, Clause 3: "Congress shall have Power…. To regulate Commerce with foreign nations, and

[103] *Id.*
[104] *Id.*
[105] U.S. Const. amend. X states: 'The powers not delegated to the United States by the Constitution, nor prohibited by it to the states, are reserved to the states respectively, or to the people.
[106] U.S. Const. art. I, § 8, cl. 3.

among the several States, and with the Indian Tribes."[107] The Supreme Court on numerous occasions has interpreted the Commerce Clause as giving Congress the authority to regulate the channels of interstate commerce, persons or things in interstate commerce, and those activities that substantially affect interstate commerce.[108]

Further, issues relating to whether Congress has the authority to regulate the private information collected by companies, and other technological industries, under the Commerce Clause, is a question that is similar to that which was addressed by the Supreme Court in *Reno v. Condon*.[109] The court in *Reno* held that pieces of personal information and data garnered by state DMVs were "things in interstate commerce" that fell under the scope of the Commerce Clause, and Congress's power.[110] Further, the Court also held that the Tenth Amendment does not apply when the regulation of the disclosure and selling of private information is applied evenly to both state and private holders of the information.[111] Applying the logic of the Supreme Court in *Reno* here, personal information collected by private companies, the individual, and states through the metaverse, could be subject to regulation, under *Reno's* precedent. This means that Congress could enact a federal framework without there being an issue of constitutionality raised if the application of the law impacts both States and private individuals similarly. Here, because the regulation regarding the collection of data impacts how both states and private individuals can collect and monitor the storage of user data, the 10th amendment issue does not apply here.

---

[107] Michael A. Foster & Erin H. Ward, *Congress's Authority to Regulate Interstate Commerce*, CONGRESSIONAL RESEARCH SERVICE (Nov.15, 2021), https://crsreports.congress.gov/product/pdf/IF/IF11971.
[108] Edward C. Liu, *Constitutional Authority to Regulate the Privacy of State-Collected Contact-Tracing Data*, CONGRESSIONAL RESEARCH SERVICE (Jun. 26, 2020), https://crsreports.congress.gov/product/pdf/LSB/LSB10502.
[109] *Reno v. Condon*, 528 U.S. 141 (2000).
[110] *Id.*
[111] *Id.*

Further, if the Supremacy Clause[112] from the Constitution is applied, the federal framework would pre-empt any privacy regulations created under State law, which would further give Congress the authority to regulate privacy laws, without the impediment of State laws.[113] All these powers would give Congress the right to create a federal privacy framework, similar to that which exists in the EU, that would be upheld.

C. Challenges to Creating a National Privacy Law: The Issues of the Free Market

Another major issue is whether Congress would even want to enact a federal framework of privacy because many major companies and industries have made fortunes in the absence of privacy regulations. More specifically, many companies are able to buy and sell private information that enables them to accurately market their goods to consumers.[114] Those who are against creating a national framework will argue that the transferring and exchanging of information has allowed innovation and growth within the industry, allowing for the spread of different ideas across platforms.[115] Conversely, there are two counterarguments that can be made: (1) although the spread of personal data has created a more free market for companies, it has also encouraged deceptive marketing practices and the increase of crime within these spaces, which has led to the violation of many individuals' privacy rights, and the lack of understanding/ consent as to the storage, surveillance, collection, and sale of private information; and (2) some

[112] U.S. Const. art. VI, C2.1 (establishing that the Supremacy clause of the Constitution provides that federal law takes precedence over state law).
[113] U.S. Const. art. VI, cl. 2. ("This Constitution, and the Laws of the United States which shall be made in Pursuance thereof; and all Treaties made, or which shall be made, under the Authority of the United States, shall be the supreme Law of the Land; and the Judges in every State shall be bound thereby, any Thing in the Constitution or Laws of any State to the Contrary notwithstanding.").
[114] Mark Andrus, *The New Oil: The Right to Control One's Identity in Light of the Commoditization of the Individual*, ABA BLT (Sept. 19, 2018), https://www.americanbar.org/groups/business_law/publications/blt/2017/09/06_andrus/.
[115] *Id.*

of those companies will actually benefit from a federal law that is similar to the EU's framework because it will allow for uniformity and the development of closer relationships with consumers.

In the metaverse, there will be large amounts of personal data being stored; without privacy regulations, deceptive practices will be encouraged, and criminal privacy violations will not be stopped or controlled. Consumers and users deserve to be aware of the depth of information that is being taken without their consent. According to the Pew Research Center, " 68% of American internet users believe current laws are not good enough in protecting people's privacy online."[116] Thus, although one can make an argument in favor of the free market, and the spread of technological growth, the government should step in whenever there is substantial harm to a fundamental right.[117] Aside from the right to privacy, many companies will benefit from a federal framework because (1) it allows them to follow a unified set of guidelines; and (2) research has shown that effective privacy laws can help businesses grow, and that organizations within the EU have had major success with their privacy laws without an effect on their market.

First, preemption of state laws for a federal privacy framework will avoid the cost of complying with a jumble of laws because there will be unified regulations and standards that are enforced across the board.[118] Moreover, with many countries in Europe already following stricter privacy regulations, larger companies will have an easier time complying with GDPR laws and US laws if they are more similar- it will allow for an improved portability of information.[119] Secondly, research has shown that many businesses benefit from effective privacy laws, because

---

[116] *The state of privacy in post-Snowden America*, PEW RESEARCH (September 21, 2016), https://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/.
[117] Dawin Brown*, Americans are more concerned with data privacy than job creation, study shows*, USA TODAY (November 9, 2018), https://www.usatoday.com/story/money/2018/11/09/americans-more-concerned-data-privacythan-healthcare-study-says/1904796002/.
[118] Tony Glosson, *Data Privacy in Our Federalist System: Toward an Evaluative Framework for State Privacy Laws*, 67 FED. COMM. L.J. 409, 415 (2015).
[119] *Id.*

consumers were more likely to interact and spend more money on organizations that they believed better protected their personal data, and followed a specific set of guidelines for protecting them.[120] In other words, when consumers knew they were protected by privacy laws, they were likely to favor companies that were obligated to follow them. [121] The same study highlighted that compliance with privacy regulations builds brand loyalty and trust with consumers.[122] European companies have even seen an increase in customer- company relationships, due to better treatment and conversations with customers, and increased transparency.[123] Ultimately, what we have seen through the EU is that a federal framework for privacy might be encouraged amongst companies.

D. The Enforcement of a National Privacy Law

The final issue that arises with implementing a federal privacy framework to regulate the metaverse, is how enforcement of the regulations would occur. Although some argue for a new agency to be created to enforce the privacy laws, there is already an agency that has the ability, the funding, and the power to do so.[124] The Federal Trade Commission (FTC) is an independent U.S. law enforcement agency that is delegated with protecting consumers across broad sectors of the economy.[125] The FTC's legal power comes from Section 5 of the Federal Trade Commission Act, which bars unfair, illegal, or deceptive practices in the marketplace.[126] The FTC has already

[120] Adam Uzialko, *How GDPR Is Impacting Business and What to Expect in 2020*, BUSINESS NEWS DAILY (Aug. 05, 2022), https://www.businessnewsdaily.com/15510-gdpr-in-review-data-privacy.html.
[121] *Id.*
[122] Id.
[123] *Id* (highlighting that by increasing transparency in a company's privacy policy, consumers will trust the company more, and will, in turn, establish stronger relationships with the company).
[124] Michael Scully & Cobun Keegan*, IAPP Guide to FTC Privacy Enforcement*, IAPP (2017), https://iapp.org/media/pdf/resource_center/Scully-FTC-Remedies2017.pdf.
[125] *Privacy & Data Security Update: 2018*, FEDERAL TRADE COMMISSION (2018), https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2018/2018-privacy-data-security-report-508.pdf.
[126] *Id.*

been given the power to implement a federal framework protecting privacy, as their main job has always been to protect consumers from any harmful or criminal practices by companies or individuals; which includes the stealing of their biometric and personal data.[127] If there is a federal privacy framework, the FTC would be given the authority to regulate business and individual compliance with privacy regulations within the metaverse and punish those that break the rules. Some of their powers include, "when appropriate, implementation of comprehensive privacy and security programs, biennial assessments by independent experts, monetary redress to consumers, disgorgement of ill-gotten gains, deletion of illegally obtained consumer information, and providing robust transparency and choice mechanisms to consumers."[128] The FTC can also seek civil monetary damages for violations and bring class actions against companies.[129] Finally, the FTC has the power under section 45 of the Federal Trade Commission Act, to bring charges against individuals who cause harm to consumers through fraud, money laundering, or identity theft, because their power applies to both cybersecurity and privacy policies.[130]

Because the FTC is equipped with the capability to control privacy regulations amongst individuals and companies, consumers will be able to gain control over their own information, and thus will have more privacy.[131] An increase in privacy amongst consumers will mean that cybercrimes (such as identity theft, terrorism, money laundering, and/or child harassment) will decrease because it will be harder for individuals to get access to the biometric and personal data needed to commit these crimes.[132] With a bigger and more robust privacy framework, the FTC

[127] *Id.*
[128] *Id.*
[129] *Id.*
[130] F.T.C. v. Wyndham Worldwide Corp*.,* 799 F.3d 236, 249 (2015).
[131] Michael Scully*, IAPP Guide to FTC Privacy Enforcement*, IAPP (Mar. 1, 2023), https://iapp.org/media/pdf/resource_center/Scully-FTC-Remedies2017.pdf .

[132] *Id.*

will have broader power to enact and enforce these regulations, similar to the manner in which the EU does, and control large scale privacy violations, especially within the metaverse.

IV. Conclusion

The metaverse is a new technological advancement which will unquestionably grow in the next few months and years. As more companies and individuals join, there becomes a greater threat of unregulated access to an extraordinary amount of private data. Due to the lack of an existing federal privacy framework in the United States, that threat grows stronger, as more companies and criminals will benefit off stealing user's information for their own profit and exploiting individual's privacy. Further, many individuals that have access to the data of others can use that information for the continuation of criminal activity at a level that has not been explored yet.

For there to be a solution to this problem, the US must look towards the EU when implementing a framework. Specifically, Congress should look to their ideals of transparency, which are reflected in three important rules (1) companies and individuals should be controlled from selling individual's data without consent; (2) there must be an enforcement mechanism that monitors each company; and (3) the data protection should include regulation of biometric data, targeted advertisement, and criminal activity. Although it might seem demanding, neither the Constitution nor other companies would serve as a barrier to this type of framework. For this reason, Congress should attempt to do what they can to look forward and create a structure that protects individuals against predatory privacy violations, specifically those that will occur within the metaverse. With the advancement of the metaverse, a world without privacy regulations in it,

would look eerily similar to a world in a science fiction novel, where the idea of privacy ceases to exist.