FUTURE OF PRIVACY FORUM

1350 Eye Street NW, Suite 350, Washington, DC 20005 | 202-768-8950 | fpf.org

Filed online at regulations.gov

April 29, 2024

Ms. April Tabor
Secretary
Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue, NW
Suite CC-5610 (Annex E)
Washington, D.C. 20580

Re: Proposed Amendments to Trade Regulation Rule on Impersonation of Government and Businesses ("Impersonation SNPRM")

The Future of Privacy Forum (FPF) welcomes the opportunity to submit comments in response to the Federal Trade Commission's (FTC, or Commission) Supplemental Notice of Proposed Rulemaking (SNPRM). In the SNPRM, the FTC proposes amending the Trade Regulation Rule on Impersonation of Government and Businesses (Impersonation Rule, or Rule), which was finalized on February 15, 2024 under Section 18 of the FTC Act (Magnuson-Moss), to add a prohibition on the impersonation of individuals.[1] FPF is a global non-profit organization dedicated to advancing privacy leadership, scholarship, and principled data practices in support of emerging technologies.

The growth of widely-available artificial intelligence (AI) tools has brought both exciting benefits as well as heightened opportunities for malicious impersonation. The risks associated with AI-enabled impersonation may be further exacerbated by the expansion of immersive technologies, including extended reality, spatial computing, and neurotechnologies.[2] In recognition of this context, FPF supports a trade regulation rule covering impersonation of individuals. In doing so, FPF also makes the following recommendations:

I. The FTC's prohibition on impersonation of individuals in commerce should cover risks posed by new technologies, including generative AI and immersive technologies.

[1] Federal Trade Commission, *Supplemental notice of proposed rulemaking; request for public comment: Trade Regulation Rule on Impersonation of Government and Businesses* (Mar. 1, 2022), https://www.federalregister.gov/documents/2024/03/01/2024-03793/trade-regulation-rule-on-impersonation-of-government-and-businesses.

[2] For the purposes of this comment, FPF uses the terms "immersive technologies" and "immersive environments" to refer generally to a collection of hardware and software products that substitute, enhance, or alter users' individual, physical-world experiences. This includes extended reality (XR), virtual world and social gaming applications, neurotechnologies, and other related technologies.

II. To the extent it has the authority, the FTC should address identity-based harms to individuals whose information is misused to facilitate impersonation.

III. If the FTC expands liability for Rule violations to parties who provide "means and instrumentalities" for impersonation, it should:

   A. Consider the potential impacts of applying a constructive knowledge standard or an actual knowledge standard.

   B. Provide recommendations, best practices, or tools for good faith parties to comply with the requirements of the Rule.

Background: Widely-available AI tools increase the risk of impersonation of individuals, which can be addressed through regulation.

Advances in AI have made video and voice manipulation techniques easier to use and more realistic than ever before. At the same time, these tools are being made widely available to the public. Like any powerful technology, sophisticated AI tools have both beneficial and harmful uses—including, in this case, the heightened ability to perpetrate fraud, identity theft, and impersonation.

For example, generative AI (GenAI), which refers to machine learning models that analyze existing data in order to create new text, audio, video, and other media, has grown rapidly in popularity in the last few years.[3] While GenAI may improve outcomes in healthcare, education, productivity, and more, it also poses a number of risks to individuals, communities, and society at large.[4] Notably, GenAI provides widespread, public access to tools that can accurately mimic "real," organic content such as photos, videos, or recordings of actual people. As a result, GenAI may facilitate identity theft, impersonation, fraud, and disinformation, resulting in increased personal harm, financial loss, and the weakening of societal institutions.[5]

While most developers create policies forbidding certain harmful uses of their systems, by lowering the barrier to entry for developers and content creators, new methods for maliciously capturing an entity or person's likeness—commonly known as "deepfakes"—makes it relatively simple to impersonate voices for ransom scams, create synthetic intimate imagery, or generate

[3] Adam Zewe, *Explained: Generative AI*, MIT News (Nov. 9, 2023), https://news.mit.edu/2023/explained-generative-ai-1109.

[4] Brenda Leong and Dr. Sara R. Jordan, *The Spectrum of Artificial Intelligence*, Future of Privacy Forum (June 2023), https://fpf.org/wp-content/uploads/2023/07/FPF-AIEcosystem-Report-Jun23-R4-Digital.pdf.

[5] Emilio Ferrara, *GenAI against humanity: nefarious applications of generative artificial intelligence and large language models*, Journal of Computational Social Science (Feb. 22, 2024), https://link.springer.com/article/10.1007/s42001-024-00250-1.

videos for political gain or sabotage.[6] For example, "deliberately deceptive AI-generated campaign ads" could falsely attribute statements or actions to political candidates, leading to misinformation, harassment, or voter suppression, particularly for marginalized communities.[7]

As these technologies grow in popularity, instances of impersonation—of businesses, government, and individuals—will likely increase. Some experts contend this issue will also worsen over time, noting that technical improvements in image resolution may make deepfakes essentially indistinguishable from organic content, even to high-quality detectors.[8] In addition, there are no universal regulatory, technical, or community standards around deepfakes for individual creators or online platforms.[9]

A prohibition on impersonation of individuals is likely to particularly benefit people from marginalized communities, who disproportionately suffer the harms associated with impersonation. Women, people of color, and LGBTQ+ individuals are more likely to be victims of nonconsensual explicit imagery, including synthetic intimate imagery that appropriates their likeness.[10] Additionally, marginalized individuals and communities are often targeted by disinformation campaigns, including the use of deepfakes and impersonation, intended to suppress their participation in civic life.[11]

Expanding the Impersonation Rule to include impersonation of individuals will give regulators an important tool for addressing these challenges as the technology ecosystem evolves. It will also

[6] Will Knight, *Even the AI Behind Deepfakes Can't Save Us From Being Duped*, WIRED (Oct. 2, 2019), https://www.wired.com/story/ai-deepfakes-cant-save-us-duped/. *See also* Pranshu Verma, *They Thought Loved Ones Were Calling for Help. It Was an AI Scam.*, The Washington Post (Mar. 5, 2023), https://www.washingtonpost.com/technology/2023/03/05/ai-voice-scam/. *See also* Caroline Haskins, *A Deepfake Nude Generator Reveals a Chilling Look at Its Victims*, WIRED (Mar. 25, 2024), https://www.wired.com/story/deepfake-nude-generator-chilling-look-at-its-victims/. *See also* Stuart A. Thompson, *Making Deepfakes Gets Cheaper and Easier Thanks to A.I.*, The New York Times (Mar. 12, 2023), https://www.nytimes.com/2023/03/12/technology/deepfakes-cheapfakes-videos-ai.html. *See also* Charlotte Klein, *"This Will Be Dangerous in Elections": Political Media's Next Big Challenge Is Navigating AI Deepfakes*, Vanity Fair (Mar. 6, 2023), https://www.vanityfair.com/news/2023/03/ai-2024-deepfake.

[7] Amber Ezzell, *Comment to the FEC Re: REG 2023-02 Artificial Intelligence in Campaign Ads*, Future of Privacy Forum, https://fpf.org/wp-content/uploads/2023/10/Future-of-Privacy-Forum-FEC-Comment-on-AI-in-Campaign-Ads-October-16-2023.pdf.

[8] Todd C. Helmus, *Artificial Intelligence, Deepfakes, and Disinformation: A Primer*, RAND Corporation (July 6, 2022), https://www.rand.org/pubs/perspectives/PEA1043-1.html.

[9] Shannon Bond, *AI-Generated Deepfakes are Moving Fast. Policymakers Can't Keep Up*, NPR (Apr. 27, 2023), https://www.npr.org/2023/04/27/1172387911/how-can-people-spot-fake-images-created-by-artificial-intelligence.

[10] Danielle Keats Citron, *The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age*, W.W. Norton (2022), pg. 39.

[11] Samuel Woolley, *In Many Democracies, Disinformation Targets the Most Vulnerable*, Center for International Governance Innovation (Jul. 18, 2022), https://www.cigionline.org/articles/in-many-democracies-disinformation-targets-the-most-vulnerable/.

provide another mechanism for protecting people from online impersonation when other avenues prove ineffective. Procedural hurdles make it difficult for victims of impersonation (those whose identities are misappropriated) to obtain adequate relief through the right to privacy and the right of publicity,[12] currently the main legal avenues for addressing impersonation. The decentralized nature of Internet servers has challenged courts' notions of personal jurisdiction, making enforcement difficult. At the same time, strict subpoena standards often protect defendants' online anonymity, and Section 230 of the Communications Decency Act largely shields Internet service providers from liability for third-party content.[13]

a. Use case: AI and immersive technologies may create more opportunities for malicious impersonation

While AI on its own provides new capabilities for actors seeking to engage in impersonation, it can become even more powerful when combined with other emerging technologies, including immersive technologies. People are increasingly spending more time online, using digital tools for work, school, entertainment, and social interaction. The shift to digital has brought about new ways for people to express their identities, allowing them to create virtual representations such as "avatars" that interact with others online.[14]

Virtual forms of identity, while not new, become particularly important in immersive environments, as the effectiveness of these spaces relies on users feeling like they're embedded within the virtual world.[15] Avatars can range in appearance from cartoonish to lifelike, and from human to non-human.[16] They allow users not only to experiment with their own self-expression, but also to build relationships with others while engaging in online activities.[17] The personas that people create with their avatars can thus have significant personal meaning, and are key to creating safe,

[12] For more on the distinction between victims of impersonation and victims of impersonation-driven scams, see Recommendation II.

[13] Jesse Lake, *Hey, You Stole My Avatar!: Virtual Reality and Its Risks to Identity Protection*, Emory Law Journal, Vol. 49 Issue 4 (2020), https://scholarlycommons.law.emory.edu/cgi/viewcontent.cgi?article=1016&context=elj.

[14] Jinghuai Lin and Marc Erich Latoschik, *Digital body, identity and privacy in social virtual reality: A systematic review*, Frontiers in Virtual Reality, Vol. 3 (2022), https://www.frontiersin.org/articles/10.3389/frvir.2022.974652/full.

[15] "[Immersive] technology is characterized by the existence of immersion—the user feeling as if he or she is actually in the virtual world; presence—the user experiencing the virtual world as real; and embodiment—the user embodying an avatar and treating its experiences as his or her own." *See* Brittan Heller, *Watching Androids Dream of Electric Sheep: Immersive Technology, Biometric Psychography, and the Law*, Vanderbilt Journal of Entertainment & Technology Law Vol. 23 Issue 1 (2020), https://scholarship.law.vanderbilt.edu/cgi/viewcontent.cgi?article=1000&context=jetlaw.

[16] *Supra* 13.

[17] Divine Maloney, Guo Freeman, and Andrew Robb, *Social Virtual Reality: Ethical Considerations and Future Directions for An Emerging Research Space*, 2021 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops, https://guof.people.clemson.edu/papers/ieee21.pdf.

engaging, and inclusive spaces.[18] At the same time, as avatars become more realistic—including photo-realistic 3D avatars in immersive spaces—they can also function as identifiers. Notably, the FTC has previously made clear that avatars generated from images of children are protected under the Children's Online Privacy Protection Act (COPPA).[19]

The advent of more sophisticated digital forms of representation like avatars has created new opportunities for identity theft and impersonation, in both immersive environments and online spaces more broadly. AI has accelerated the ability to create realistic avatars on demand, including deepfakes, which can facilitate impersonation leading to fraud, IP theft, data breaches, financial loss, espionage, and disinformation.[20] For example, a malicious actor could create an avatar that appropriates another person's face, voice, or other personal information, which can cause emotional, reputational, or economic damage.[21]

Due to their more realistic, embodied nature, there is reason to believe immersive technologies may be more prone to impersonation attacks than other online spaces. Studies have shown that people may have difficulty distinguishing human faces from computer-generated faces, and even find computer-generated faces *more* trustworthy than real ones.[22] Experiences in immersive environments can be so visceral that people forget the content they're interacting with is virtual, not physical.[23] The large amounts of personal data available on the Internet also make it easier to create convincing impersonations in immersive environments.[24] As a result, AI-driven impersonations and disinformation campaigns may be more effective in immersive environments, creating both individual and societal-level risks.

While empirical data on the prevalence of impersonation in immersive environments is scarce, anecdotal evidence, as well as studies from other similar sectors, indicate this is a growing problem. Immersive technologies' relative novelty, and lack of current widespread adoption, has

[18] World Economic Forum and Accenture, *Metaverse Identity: Defining the Self in a Blended Reality* (Mar. 2024), https://www3.weforum.org/docs/WEF_Metaverse_Identity_Defining_the_Self_in_a_Blended_Reality_2024.pdf.

[19] Federal Trade Commission, *FTC Will Require Microsoft to Pay $20 million over Charges it Illegally Collected Personal Information from Children without Their Parents' Consent* (Jun. 5, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/06/ftc-will-require-microsoft-pay-20-million-over-charges-it-illegally-collected-personal-information.

[20] Shahroz Tariq, Alsharif Abuadbba, and Kristen Moore, *Deepfake in the Metaverse: Security Implications for Virtual Gaming, Meetings, and Offices*, WDC '23: Proceedings of the 2nd Workshop on Security Implications of Deepfakes and Cheapfakes (2023), https://dl.acm.org/doi/abs/10.1145/3595353.3595880.

[21] Ellysse Dick, *Balancing User Privacy and Innovation in Augmented and Virtual Reality*, ITIF (Mar. 4, 2021), https://itif.org/publications/2021/03/04/balancing-user-privacy-and-innovation-augmented-and-virtual-reality.

[22] Louis Rosenberg, *Evil twins and digital elves: How the metaverse will create new forms of fraud and deception*, Big Think (Apr. 25, 2022), https://bigthink.com/the-future/metaverse-fraud-digital-twins/.

[23] Jameson Spivack and Daniel Berrick, *Immersive Tech Obscures Reality. AI Will Threaten It*, WIRED (Sep. 27, 2023), https://www.wired.com/story/immersive-technology-artificial-intelligence-disinformation/.

[24] *Supra* 29.

meant the technologies are understudied in general, particularly in regards to impersonations.[25] That said, identity theft has been documented in virtual worlds, as have other types of fraud.[26] Additionally, the prevalence of impersonations in other similar online environments—such as gaming, social media, and dating apps—suggests that this is likely a problem in immersive spaces as well, particularly given their realistic nature.[27]

Recommendation I: The FTC's prohibition on impersonation of individuals in commerce should cover risks posed by emerging technologies, including generative AI and immersive technologies.

Since the COVID-19 pandemic, online and digital social interaction has significantly increased. People are spending more time using online tools for work, school, entertainment, communication, and healthcare. At the same time, companies are investing more in emerging technologies, including AI tools, as well as in immersive computing, media, and "metaverse" applications like extended reality (XR) and virtual world platforms.[28] As described above, these technologies provide new and potentially more effective opportunities to engage in impersonation of individuals.

While the SNPRM provides helpful illustrative examples of activities that would run afoul of the proposed Rule, the examples don't adequately capture the risks that emerging technologies may pose. Though the list is intentionally non-exhaustive, it would be helpful to also acknowledge some of the ways impersonation is manifesting in emerging technologies. For example, this could include behavior such as creating an avatar or digital representation of another person based on their voice or likeness for fraud or manipulation, or developing written material that intentionally imitates another identified individual's style or tone for deceptive purposes.[29] In both providing

[25] *Supra* 13.

[26] William N. Dilla, Andrew J. Harrison, Brian E. Mennecke, and Diane J Janvrin, *The Assets Are Virtual but the Behavior Is Real: An Analysis of Fraud in Virtual Worlds and Its Implications for the Real World*, Journal of Information Systems, Vol. 27 Issue 2 (Dec. 2013), https://www.researchgate.net/publication/274071335_The_Assets_Are_Virtual_but_the_Behavior_Is_Real_An_Analysis_of_Fraud_in_Virtual_Worlds_and_Its_Implications_for_the_Real_World.

[27] For examples in gaming, *see* Moshe Leder and Gabi Stapel, *Why Attackers Target the Gaming Industry*, Imperva (May 30, 2023), https://www.imperva.com/blog/cyber-attacks-gaming-industry/. For examples in social media, *see* Jessica Ryan, *Dramatic Increase Detected in Impersonation Attacks on Social Media*, Fortra PhishLabs (Jun. 2, 2022), https://www.phishlabs.com/blog/dramatic-increase-detected-in-impersonation-attacks-on-social-media. For examples in dating apps, *see* Emma Fletcher, *Reports of romance scams hit record highs in 2021*, FTC Consumer Protection Data Spotlight (Feb. 10, 2022), https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/02/reports-romance-scams-hit-record-highs-2021.

[28] *Supra* 13.

[29] Avatars or other digital representations that incorporate the likeness of real people—whether appearance, voice, or other characteristics—could be used to deceive or manipulate. For example, an avatar that mimics a person's loved one will be more effective at persuading them to buy certain products, vote for particular candidates, or believe information.

compliance guidance to companies and in engaging in enforcement, the FTC should consider the unique ways that emerging technologies like AI and immersive tech can facilitate harmful impersonation.

Recommendation II: To the extent it has the authority, the FTC should address identity-based harms to individuals whose information is misused to facilitate impersonation.

As proposed, the expanded Rule would cover not just impersonations of "real" individuals but "fictitious" ones as well, specifically recognizing the prevalence of romance scams in which an impersonator poses as a fictitious potential romantic partner. Distinguishing between these two different types of impersonation is important for several reasons.

First, while there is certainly overlap, the people impacted by each type of impersonation—and the harms they experience—may be different. Fictitious impersonation involves one party being harmed: the victim of an impersonation-driven scam, who has been tricked into giving up money, personal information, or other valuables. Real impersonation, on the other hand, involves two harmed parties: the victim of an impersonation-driven scam *and* the victim of impersonation themselves, whose identity is stolen or misappropriated. Both can be subjected to financial, reputational, and emotional injury, though these harms may manifest differently. Scam victims may be duped into giving their money or personal information up to a thief, and may feel violated by or embarrassed about being tricked. Impersonation victims may suffer reputational damage or unauthorized access to their accounts, and may also feel violated by someone posing as them.[30] The Impersonation Rule clearly covers victims of impersonation-driven scams; to the extent the FTC has the jurisdictional authority to do so, it should also protect victims of impersonation as well.

Second, while fictitious impersonation can and often does result in harmful, fraudulent activity, an over-broad conception could discourage or even proscribe protected anonymous or pseudonymous speech online. Unlike impersonation of real individuals, which is inherently harmful to those being impersonated (and potentially to others as well), fictitious impersonation is only directly harmful when used to scam or defraud someone. As described above, avatars and alternative forms of identity have grown in popularity in online spaces, providing people with the ability to both explore their identities and engage in anonymous speech. Read broadly, a prohibition on fictitious impersonation could apply to the mere act of creating an online persona that does not match the user's physical world identity.[31] The FTC should be clear that fictitious

[30] Danielle Keats Citron and Daniel J. Solove, *Privacy Harms*, Boston University Law Review, Vol. 102 (2022), https://www.bu.edu/bulawreview/files/2022/04/CITRON-SOLOVE.pdf.

[31] Given the importance of avatars to transgender individuals, there may also be a disparate impact on trans and gender diverse people. *See* Helen Morgan, Amanda O'Donovan, Renita Almeida, Ashleigh Lin, and Yael Perry, *The Role of the Avatar in Gaming for Trans and Gender Diverse Young People*, International Journal of Environmental Research and Public Health, Vol. 17 Issue 22 (2020), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7699515/.

impersonation involves not merely creating an alternate identity online, but also using this identity to engage in behavior that defrauds another person to cause specific harm. In the SNPRM, the FTC demonstrated a number of instances in which individual impersonation led to harm; similarly, it should clarify that prohibited fictitious impersonation is that which results in identified harms.

Recommendation III(A): If the FTC expands liability for Rule violations to parties who provide "means and instrumentalities" for impersonation, it should consider the potential impacts of applying either a constructive knowledge standard, as proposed, or an actual knowledge standard.

In its Notice of Proposed Rulemaking (NPRM), the Commission proposed making it unlawful to provide the "means and instrumentalities" for impersonation in violation of the Impersonation Rule.[32] A number of comments in response to the NPRM raised questions about the potential impact of extending liability to actors who provide "means and instrumentalities," which may be interpreted to impose strict liability on good faith companies unaware their services are used for impersonation.[33] In response to comments, the Commission has proposed extending liability to those "with knowledge or reason to know" their services are used for impersonation (henceforth, a "constructive knowledge" standard).[34] The Commission should consider the potential consequences of adopting either a constructive knowledge standard or an actual knowledge standard, and provide additional information to entities on how they may best comply with the requirement.

a. *Knowledge Standards*

i. *Constructive knowledge*

The constructive knowledge standard applies to entities "with knowledge or reason to know" how their products may be used. This standard may be seen as representing a middle ground

[32] Federal Trade Commission, *Notice of proposed rulemaking; request for public comment: Trade Regulation Rule on Impersonation of Government and Businesses* (Oct. 17, 2022), https://www.federalregister.gov/documents/2022/10/17/2022-21289/trade-regulation-rule-on-impersonation-of-government-and-businesses.

[33] NetChoice, *Comment regarding FTC Business Impersonation Rule Comment* (2022), https://www.regulations.gov/comment/FTC-2022-0064-0053. *See also* ZoomInfo Technologies, *FTC Comments on Business Impersonation Rulemaking* (2022), https://www.regulations.gov/comment/FTC-2022-0064-0079. *See also* Consumer Technology Association, *Government and Business Impersonation Fraud NPRM Comments* (2022), https://www.regulations.gov/comment/FTC-2022-0064-0063. *See also* Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG), *FTC Comments on Impersonation* (2022), https://www.regulations.gov/comment/FTC-2022-0064-0051.

[34] Federal Trade Commission, *Proposed Amendments to Trade Regulation Rule on Impersonation of Government and Businesses* (2024), https://www.ftc.gov/system/files/ftc_gov/pdf/r207000_impersonation_snprm.pdf.

between applying what is essentially strict liability and a more narrow actual knowledge standard, and has been applied and explicated in other federal regulations.[35]

ii. Actual knowledge

In response to the Commission's NPRM, a number of commenters called for the adoption of an actual knowledge standard, which would apply to entities only if they are aware or intentionally ignorant of the fact that their product is being used for impersonation.[36] The FTC's Telemarketing Sales Rule adopts such a standard, holding liable entities that "provide substantial assistance or support to any seller or telemarketer when that person *knows or consciously avoids knowing*" (emphasis added) that the seller or telemarketer is violating the Rule.[37] This is also the standard found in COPPA in regard to information collected from a child,[38] as well as Section 5 of the FTC Act in regard to unfair and deceptive acts or practices.[39]

iii. Actual knowledge ("bad faith" variant)

A variation of the actual knowledge standard would only hold entities liable when they "knowingly and intentionally" provided means and instrumentalities for impersonation,[40] or did so "wilfully or in bad faith" or "with clear intent and specific knowledge."[41] In such a case, an entity doesn't merely know about its product being used for impersonation, but also plays an active role in facilitating it.

b. The FTC should more fully examine the consequences of adopting any knowledge standard and provide additional information on compliance.

[35] 26 CFR § 53.4965-6 - Meaning of "knows or has reason to know," https://www.law.cornell.edu/cfr/text/26/53.4965-6. *See also* 13 CFR § 142.6 - What does the phrase "know or have reason to know" mean?, https://www.law.cornell.edu/cfr/text/13/142.6.

[36] Consumer Technology Association, *Government and Business Impersonation Fraud NPRM Comments* (2022), https://www.regulations.gov/comment/FTC-2022-0064-0063. *See also* Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG), *FTC Comments on Impersonation* (2022), https://www.regulations.gov/comment/FTC-2022-0064-0051.

[37] Federal Trade Commission, *Telemarketing Sales Rule*, https://www.ftc.gov/legal-library/browse/rules/telemarketing-sales-rule.

[38] Federal Trade Commission, *Complying with COPPA: Frequently Asked Questions*, https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions.

[39] Federal Trade Commission, *A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority* (May 2021), https://www.ftc.gov/about-ftc/mission/enforcement-authority.

[40] This would mirror the "actual malice" standard found in defamation law. *See* ZoomInfo Technologies, *FTC Comments on Business Impersonation Rulemaking* (2022), https://www.regulations.gov/comment/FTC-2022-0064-0079.

[41] Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG), *FTC Comments on Impersonation* (2022), https://www.regulations.gov/comment/FTC-2022-0064-0051.

The Commission should fully consider all potential consequences related to expanding liability to entities providing “means and instrumentalities” for the impersonation of individuals. In particular, for standards that require an organization to judge a user’s intent in using their services, the Commission should consider how such a standard should best be applied without increasing other risks. For instance, any knowledge standard requiring entities to anticipate misuse of their products will require additional data collection from, or monitoring of, its users, potentially raising privacy risks.[42] In the case of AI developers, it may not be possible to fully anticipate all harmful downstream uses of their products.

If the Commission expands liability, it should also provide additional details on and examples of behavior that may run afoul of the Rule, regardless of which knowledge standard is used. Notably, of the aforementioned knowledge standards, “actual knowledge” offers the most precise standard for entities determining how to comply with the new Rule. Even in the case of a “bad faith” actual knowledge standard, of which the Commission has already provided an example in the text of the NPRM,[43] additional clarifying information in the context of online platforms and services would clear up uncertainty around what conduct would violate the Rule.

Recommendation III(B): If the FTC expands liability for Rule violations to parties who provide “means and instrumentalities” for impersonation, it should provide recommendations, best practices, or tools for good faith parties to comply with the requirements of the Rule.

Regardless of what knowledge standard the Commission adopts in regards to providing “means and instrumentalities” for impersonation, it should provide appropriate tools for ensuring compliance with the Rule. For instance, the FTC may consider developing best practices or recommendations to assist in combating identity theft and impersonation in immersive products or services, including technical approaches that organizations can adopt. This could include user authentication, as well as avatar authentication, which matches avatars to their human counterparts across virtual worlds. Additionally, strong user access controls, identity management, and privacy mechanisms can protect against impersonations.[44] Finally, explicit

[42] For example, laws mandating age verification of users requires entities to collect more data about users. *See* David Sallay, *FPF Analysis on Utah Legislation*, Future of Privacy Forum (2023), https://fpf.org/wp-content/uploads/2023/02/FPF-Analysis-on-Utah-legislation.pdf.

[43] “An example of a violation of proposed §461.4's prohibition on providing the means and instrumentalities for impersonation is a person who fabricates official-looking Internal Revenue Service (IRS) Special Agent identification badges for sale. In this example, the person does not actually impersonate an IRS Special Agent, so does not violate proposed §461.2's prohibition against impersonating government officers but does provide the means and instrumentalities for others to do so, which violates proposed §461.4.” *See* Federal Trade Commission, *Notice of proposed rulemaking; request for public comment: Trade Regulation Rule on Impersonation of Government and Businesses* (Oct. 17, 2022), https://www.federalregister.gov/documents/2022/10/17/2022-21289/trade-regulation-rule-on-impersonation-of-government-and-businesses.

[44] Jinghuai Lin and Marc Erich Latoschik, *Digital body, identity and privacy in social virtual reality: A systematic review*, Frontiers in Virtual Reality, Vol. 3 (2022), https://www.frontiersin.org/articles/10.3389/frvir.2022.974652/full.

disclaimers of AI use, labeling, and watermarks can provide transparency that make impersonations easier to spot.[45] Many large digital platforms already employ tools to track illegal behavior online, and industry standards—for both developers and deployers of AI[46]—could be updated to account for immersive environments.

At a minimum, the FTC should develop guidance for covered entities addressing the following questions:

- **What factors would put an entity in a position in which they "have reason to know" their services are being used for impersonation?** For example, does belonging to a particular category of service or application that is vulnerable to impersonations constitute a "reason to know"?
- **What factors would constitute "actual knowledge"?** For example, does receiving reports of impersonations from users or individuals constitute "actual knowledge"? What actions make an organization complicit in aiding and abetting impersonation?
- **What steps should an entity take before an impersonation might occur in order to comply with the Rule?** For example, this could include instituting appropriate policies and contractual agreements, setting up processes for reporting impersonations, and instituting ID management and authentication mechanisms.
- **What steps should an entity take after an impersonation might occur in order to comply with the Rule?** For example, this could include monitoring and auditing their services for violations, investigating reports of impersonation, removing and blocking violators, and reporting violations to the FTC.

FPF appreciates the opportunity to comment on these issues, and the FTC's ongoing efforts to address the privacy and safety risks exacerbated by AI and other emerging technologies. We welcome any further opportunity to provide resources or information to assist in this vital effort. If you have any questions regarding these comments and recommendations, please contact Jameson Spivack at jspivack@fpf.org (cc: info@fpf.org).

Sincerely,

Jameson Spivack, Senior Policy Analyst, Immersive Technologies
Beth Do, Christopher Wolf Diversity Law Fellow
Angela Guo, Policy Intern

The Future of Privacy Forum
https://fpf.org/

[45] Emilio Ferrara, *GenAI against humanity: nefarious applications of generative artificial intelligence and large language models*, Journal of Computational Social Science (Feb. 22, 2024), https://link.springer.com/article/10.1007/s42001-024-00250-1.

[46] BSA | The Software Alliance, *AI Developers and Deployers: An Important Distinction* (2023), https://www.bsa.org/files/policy-filings/03162023aidevdep.pdf.