Before the
FEDERAL TRADE COMMISSION
Washington, DC 20580

In the Matter of	)	
	)	
Trade Regulation Rule on Impersonation of Government and Businesses	)	RIN 3084–AB71
	)	
	)	

COMMENTS OF PUBLIC KNOWLEDGE AND ELECTRONIC FRONTIER FOUNDATION

Public Knowledge and Electronic Frontier Foundation support the FTC's proposal "to impose liability on those who provide goods or services with knowledge or reason to know that those goods or services will be used in impersonations of the kind that are themselves unlawful under the Rule."[1] This proposal is a crucial step in combating the growing problem of impersonation scams and protecting consumers from financial and personal harm.

However, more specificity is needed in the language of the rule to ensure that general-purpose tools, which may have the potential for misuse, are not unintentionally swept in by the regulation. Many technologies, including AI tools, have both lawful and unlawful applications. It is essential that the rule targets bad actors who knowingly facilitate impersonation scams while not stifling innovation or unduly restricting the development and use of technologies with substantial legitimate uses.

I. Interpreting the Relevant Legal Standards

The standard of "knowledge or reason to know" should be defined to require actual knowledge or willful ignorance of specific unlawful uses. This interpretation will ensure that the

[1] Trade Regulation Rule on Impersonation of Government and Businesses, Supplemental Notice of Proposed Rulemaking, RIN 3084–AB71, 89 FR 15072, 15077 (2024).

sellers and developers of general-purpose tools that may be misused by bad actors are not swept in by a too broad standard.

Taken too broadly, the statement that "[o]ne who places in the hands of another a means of consummating a fraud or competing unfairly in violation of the Federal Trade Commission Act is himself guilty of a violation of the Act,"[2] would apply to far too wide a range of behavior, and will hold sellers and makers of general-purpose tools liable for misuses they cannot control. In many cases, tools cannot be fairly considered "a means of consummating a fraud" as they have significant legitimate uses.

At the same time, an instrumentality that is only suitable for unlawful activities (or nearly so) *may* be considered "a means of consummating a fraud or competing unfairly." Providing such an instrumentality with knowledge of its foreseeable intended unlawful use would likely meet the knowledge standard under the proposed rule. The courts and the FTC have consistently recognized providing means and instrumentalities that lack legitimate uses as a form of primary liability under the Section 5 of the FTC Act.[3] However, determining whether this standard is met in a particular case would require an examination of the specific facts, and the intent, knowledge, and behavior of the relevant parties. Categorical or too-broad approaches would likely unintentionally sweep in innocent parties.

In *Magui Publishers*, the district court determined that the defendants knowingly supplied deceptive artwork, certificates and promotional materials to their retail customers, fully aware

[2] *C. Howard Hunt Pen Co. v. FTC*, 197 F. 2d 273, 281 (3rd Cir. 1952).

[3] Section 5 of the FTC Act prohibits unfair or deceptive acts or practices. The proposed amendments to the Rule here will allow the Commission to seek civil penalties against the violators under Section 5.

that these customers would be used to deceive consumers.[4] Consequently, the court found that the defendants possessed the requisite "actual knowledge" to establish liability under Section 5.[5]

Similarly, in 1952, the Third Circuit held a pen manufacturer accountable for falsely labeling its pen points as "Iridium tipped," despite knowing they were not tipped with iridium.[6] The court rejected the manufacturer's defense that they were merely following their customers' instructions, applying a well-settled principle that knowingly providing the means to perpetrate fraud or unfair competition violates the FTC Act.[7]

The FTC has applied a comparable principle to establish "actual knowledge." For instance, in a 1977 case, the Commission held a wholesaler liable for the unlawful activity of its distributors because it provided them with a marketing scheme while being aware of its unlawful nature.[8] In 2000, the Commission found an auto company liable for furnishing participants in its program with materials containing false and misleading earnings claims, thereby deceiving consumers.[9]

Selling or making a general-purpose tool with the knowledge that it may *potentially* be used for lawbreaking, however, should not constitute knowledge for the purpose of this rule. Many technologies, from email to artificial intelligence, can be used for both lawful and unlawful purposes. Holding the sellers or developers of these tools liable for the misuse of their products, absent specific knowledge of unlawful use, would be detrimental to technological progress and consumer welfare.

---

[4] *FTC v. Magui Publishers*, 1991 U.S. Dist. LEXIS 20452, *43 (Mar. 28, 1991).
[5] *Id*.
[6] *C. Howard Hunt Pen Co. v. FTC*, 197 F. 2d 273, 279–80 (3d Cir. 1952).
[7] *Id*. at 281; *FTC v. Winsted Hosiery Co.*, 258 U.S. 483, 494 (1922); *see also Regina Corp. v. FTC*, 322 F.2d 765, 768 (3d Cir. 1963) (mere supplying of false documentation alone is enough to establish a violation of Section 5 of the FTC Act).
[8] *National Housewares*, 90 F.T.C. 512 (1977).
[9] *FTC v. Five-Star Auto Club*, 97 F. Supp. 2d 502, 506 (May 17, 2000).

The Commission has distinguished between two legal theories regarding the absence of specific knowledge—the means and instrumentalities theory, and the aiding and abetting theory.[10] In the *Shell* case, for example, Commissioner Swindle underscored that if Shell only provided assistance to its customers, who independently made deceptive acceleration claims to consumers, Shell could be considered an aider and abettor, thereby avoiding liability under section 5.[11]

II. Balancing the Potential for Harm and the Benefits of AI Tools

The FTC must strike a careful balance in this rulemaking between protecting consumers from the harm of impersonation scams and preserving the benefits of emerging technologies like AI. AI tools have the potential to cause harm if misused, but they also have wide-ranging beneficial applications that can improve consumers' lives.

Consider the rise of AI technology, sometimes called "deepfakes," that can create realistic-appearing images of people, or copies of their voice. Technologies like this may be useful in many areas–for example, voice cloning technology is already deployed in iPhones as an accessibility feature for users with speech impairments.[12] Technologies like this, provided they are not used misleadingly or abusively, can also be valuable in arts and entertainment. But their potential for malicious exploitation, including non-consensual pornography and political disinformation campaigns, raises urgent concerns.

---

[10] *Shell Oil Company and Shell Chemical Company*, 128 F.T.C. 749 (1999) (Commissioner Orson Swindle dissented in the Shell case in 1999, emphasizing that the Supreme Court had clearly distinguished between the two theories following the Central Bank of Denver decision. Accordingly, Commissioner Swindle argued that the Commission should assess the defendant's liability by examining the role played by the defendant in relation to the deceptive conduct transmitted to consumers by its customers.).

[11] *Id*.

[12] Edward C. Baig, *How to Clone Your Own Voice on an iPhone*, AARP (Sep. 11, 2023) https://www.aarp.org/home-family/personal-technology/info-2023/iphone-voice-cloning.html

An overly broad approach to "instrumentalities" could harm the very constituencies the Commission seeks to protect. For example, AI tools that can be used to facilitate impersonation scams can also be used to protect users from these very scams. For example, AI-powered identity verification systems can help prevent impersonation, AI-driven content moderation can identify and remove scam content from online platforms, and AI-based algorithms to detect phishing emails, fraudulent transactions or counterfeit products.[13]

Clear guidelines should delineate the permissible uses of AI tools, while holding platforms accountable for preventing and addressing impersonation scams. Policymakers must strike a balance between leveraging AI's benefits and mitigating its potential harms to effectively combat impersonation scams in the digital landscape.

III. Relevant Precedent from Other Areas of Law

Particularly when it comes to new and developing technologies, copyright and Internet law can offer useful guidance.. In *Sony*, the Supreme Court considered whether Sony could be held liable for contributory copyright infringement based on its sale of Betamax VCRs, which were capable of both infringing and non-infringing uses.[14] The Court held that distribution of a commercial product does not constitute contributory infringement if the product is "merely capable of substantial noninfringing uses."[15] The Court found that because the VCR was capable of substantial non-infringing uses, such as time-shifting of TV programs, Sony's sale of the

[13] *See, e.g.*, Press Release, TREAS, Treasury Announces Enhanced Fraud Detection Process Using AI Recovers $374M in Fiscal Year 2023 (Feb. 28, 2024), https://home.treasury.gov/news/press-releases/jy2134; Christophe Van de Weyer, *Cybersecurity Threats: How To Fight AI With AI*, FORBES (Feb. 14, 2024, 8:30 AM), https://www.forbes.com/sites/forbestechcouncil/2024/02/14/cybersecurity-threats-how-to-fight-ai-with-ai/?sh=22a1086d2bb4; Darrell M. West, John R. Allen, *How Artificial Intelligence Is Transforming The World*, BROOKINGS (April 24, 2018), https://www.brookings.edu/articles/how-artificial-intelligence-is-transforming-the-world/#_edn4.

[14] *Sony Corp. of Am. v. Universal City Studios*, 464 U.S. 417, 457 (1984).

[15] *Id*. at 442.

technology did not amount to contributory infringement.[16] The Court noted that Sony's knowledge of the potential for infringing use would not be enough, by itself, to make Sony liable[17]—some more purposeful culpable expression and conduct would be required. This demonstrates that providing a technology with infringing and non-infringing uses does not inherently constitute culpable participation in unlawful activity, so long as the legitimate uses are not insubstantial.

The Supreme Court refined this principle in *Grokster*. The Court held that "one who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties."[18] The Court focused on evidence that it believed showed that Grokster and Streamcast actively induced infringing use of their software, such as through advertising and instructing how to engage in infringement.[19]

Applying the reasoning of *Sony* and *Grokster* here, the FTC's proposed amendment to impose liability on those who provide goods or services "with knowledge or reason to know" that they will be used for unlawful impersonation strikes the right balance. Consistent with *Sony*, merely providing general-purpose tools, even with knowledge they could potentially enable some infringing uses, would not be enough to impose liability. However, following *Grokster*, providing tools with the clear purpose of fostering infringement, as evidenced by specific acts encouraging and promoting unlawful use, could appropriately lead to liability.

---

[16] *Id*. at 456.
[17] *Id*. at 439–42.
[18] *MGM Studios v. Grokster*, 545 U.S. 913, 918 (2005).
[19] *Id*.

The "knowledge or reason to know" standard ensures that only those who culpably participate in impersonation schemes, not unwitting providers of general-purpose technologies, are subject to liability under the Rule. At the same time, this standard leaves flexibility to find liability for bad actors who purposefully provide the means to commit impersonation fraud, consistent with *Grokster*'s inducement principle.

In *Taamneh*, the Court recently addressed the scope of aiding and abetting liability under the Justice Against Sponsors of Terrorism Act (JASTA).[20] The Court held that to establish aiding and abetting liability, a plaintiff must show that the defendant "consciously and culpably participate[d]" in another's wrongdoing.[21] Importantly, the Court rejected an overly broad view of aiding and abetting liability that would sweep in those who merely provided routine, widely-available services that happened to be used by wrongdoers.[22] The Court noted that "if aiding-and-abetting liability were taken too far, then ordinary merchants could become liable for any misuse of their goods and services, no matter how attenuated their relationship with the wrongdoer. And those who merely deliver mail or transmit emails could be liable for the tortious messages contained therein."[23] Instead, the Court held that the knowledge requirement considers the defendant's mental state regarding furthering the alleged illegality, explaining that aiding and abetting requires "some level of blameworthiness" and "culpable conduct."[24] It is not enough that a defendant "knew" its services were used by wrongdoers—the defendant must have consciously and culpably participated in the wrongdoing.

---

[20] *Twitter v. Taamneh*, 598 U.S. 471, 488–93 (2023)
[21] *Id*. at 493.
[22] *Id*. at 488.
[23] *Id*. at 474.
[24] *Id*. at 489–92.

Applying this standard, the FTC's proposed rule imposing liability on those who provide goods or services "with knowledge or reason to know" that they will be used for unlawful impersonation is consistent with *Taamneh*'s articulation of aiding and abetting liability. The "knowledge or reason to know" standard ensures that only those who culpably participate in impersonation schemes, not unwitting service providers or those with the general knowledge that its products or services might be abused, are subject to liability.

At the same time, the *Taamneh* decision left open the possibility that in some cases, a service provider's assistance to wrongdoers could be "so systemic and intentional"[25] as to constitute aiding and abetting of the enterprise's unlawful acts more broadly. This suggests that truly egregious misconduct by a service provider could lead to more expansive liability.

IV. Conclusion

In light of these considerations, Public Knowledge and the Electronic Frontier Foundation urge the FTC to clarify the scope of the "knowledge or reason to know" standard in the final rule. The rule should make clear that this standard requires specific knowledge or willful ignorance of unlawful use, not just general knowledge that a tool could potentially be misused.

The final rule should also explicitly state that the sale of general-purpose technologies with substantial lawful uses does not give rise to liability, even if the seller has general knowledge that some users may misuse the technology. This clarification is essential to ensure that the rule does not unduly restrict the development and availability of beneficial technologies like AI. At the same time, the rule should make clear that a seller who specifically promotes the use of a technology for unlawful impersonation, or who continues to supply a technology to a

[25] *Id*. at 474.

user with knowledge that the user is engaged in unlawful impersonation, can be held liable. This principle will ensure that bad actors who knowingly facilitate impersonation scams can be held accountable. By striking this balance, the FTC can effectively protect consumers from the harm of impersonation scams while preserving the benefits of technological innovation.

Respectfully submitted,

John Bergmayer
Legal Director
Public Knowledge

Qianda Rao
Legal Researcher
Public Knowledge

Kit Walsh
Director of AI and Access-to-Knowledge Legal Projects
Electronic Frontier Foundation

April 30, 2024