

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

Federal Trade Commission

Proposed Trade Regulation Rule and Request for Comment on the Use of
Customer Reviews and Endorsements

R311003

88 Fed. Reg. 49,364

September 29, 2023

By notice published on July 31, 2023, the Federal Trade Commission (“FTC” or “Commission”) has requested comment on a proposed rulemaking to address certain deceptive or unfair uses of reviews and endorsements.¹ The proposed trade rule would address fake reviews, including fabricated celebrity endorsements, false claims by celebrities, testimonials that misrepresent a consumer’s actual experience with a product, and review hijacking. These comments focus on endorser testimonials that proliferate unsubstantiated claims about the seller’s offerings as well as testimonials that fail to disclose an affiliate relationship between the endorser and the seller.

The Electronic Privacy Information Center (EPIC) is a public interest research center in Washington, D.C., established in 1994 to focus on public attention on emerging civil liberties issues and to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation.² EPIC has published reports and filed amicus briefs regarding technology

¹ Trade Regulation Rule on the Use of Reviews and Endorsements, 88 Fed. Reg. 49,364 (Jul. 31, 2023), <https://www.federalregister.gov/documents/2023/07/31/2023-15581/trade-regulation-rule-on-the-use-of-consumer-reviews-and-testimonials> [hereinafter NPRM].

² EPIC, *About Us* (2023), <https://epic.org/about/>.

vendors that have not substantiated their explicit crime reduction claims or implicit accuracy claims;³ has petitioned the FTC for rulemaking regarding the privacy and security of consumer data;⁴ has filed comments in support of more robust disclosures by law enforcement organizations regarding their use of surveillance technology;⁵ and has offered testimony on similar topics.⁶

EPIC files these comments in response to the Commission’s questions concerning (1) definitions proposed under § 465.1,⁷ which should explicitly include non-natural persons; and (2) its questions on the ‘know or should have known’ standard proposed under § 465.2,⁸ which should draw from the Commission’s Endorsement Guides business guidance⁹ regarding oversight of endorsers but also impose strict liability for unfair or deceptive claims. Additionally, we emphasize that (3) Amazon Ring is not an outlier in leveraging public sector endorsements.¹⁰ While Ring is a known bad actor in this space, the problem of unreliable and unregulated public sector endorsements is substantially broader.

³ See, e.g., EPIC, *Screened & Scored in the District of Columbia* 21 (Nov. 2022), <https://epic.org/screened-scored-in-dc/> (discussing unsubstantiated crime reduction claims of ShotSpotter); Br. of Amicus Curiae EPIC, Electronic Frontier Foundation, and National Association of Criminal Defense Lawyers, No. A-3078-21T1 (N.J. Super. App. Div. Sept. 26, 2022), <https://epic.org/documents/new-jersey-v-arteaga/> (discussing likely misidentifications of facial recognition systems); Br. of Amicus Curiae EPIC, No. 18-50440 (9th Cir. Mar. 28, 2019), <https://epic.org/wp-content/uploads/amicus/algorithmic-transparency/wilson/US-v-Wilson-EPIC-Amicus.pdf> (discussing unreliability of image scanning algorithm).

⁴ EPIC, *FTC Rulemaking on Commercial Surveillance & Data Security*, <https://epic.org/ftc-rulemaking-on-commercial-surveillance-data-security/> (last visited Jan. 9, 2023).

⁵ Comments of EPIC to the New York City Police Department, POST Act Disclosures (Feb. 25, 2021), <https://epic.org/documents/nypd-post-act-disclosures/>.

⁶ See, e.g., Testimony of EPIC before D.C. Council Committee on Government Operations and Facilities, Stop Discrimination by Algorithms Act (Oct. 6, 2022), <https://epic.org/documents/epic-sdaa-written-testimony/>; Testimony of EPIC before Massachusetts Joint Committee on the Judiciary, An Act to Regulate Face Surveillance (Nov. 23, 2021), <https://epic.org/documents/an-act-to-regulate-face-surveillance-massachusetts/>.

⁷ See, e.g., NPRM at questions 6–7, <https://www.federalregister.gov/d/2023-15581/p-442>.

⁸ See, e.g., NPRM at questions 8-10, <https://www.federalregister.gov/d/2023-15581/p-445>.

⁹ Fed. Trade Comm’n, *The FTC’s Endorsement Guides: What People Are Asking* (2017), <https://www.ftc.gov/business-guidance/resources/ftcs-endorsement-guides-what-people-are-asking#advertisersresponsibilities>.

¹⁰ NPRM at n.84 (“[EPIC’s] comment focused mainly on endorsements by police organizations of one product.”).

As such, we recommend that:

- (1) The Commission’s definitions for testimonials proposed under § 465.1(b) and § 465.1(e) should be broadened to explicitly include non-natural persons, such as businesses and public sector entities. Otherwise, offending companies might argue their endorsers are neither a “well-known person” under (b) nor possess “identifying personal characteristics of an individual” under either (b) or (e) and are therefore not covered under this rule.
- (2) The Commission’s liability standard proposed under § 465.2 should draw from the Commission’s Endorsement Guides business guidance, which states that the company must have a reasonable training and oversight process in place. The lack of an adequate endorser oversight program should be a per se violation of the “know or should have known” standard as that is tantamount to the company deliberately avoiding knowing. However, the company should be held strictly liable for the unfairness or deceptiveness of the claim, as an unsubstantiated claim can harm consumers every time it is made in the marketplace, and companies should not be able to evade liability for unsubstantiated claims by speaking them through the mouths of endorsers.
- (3) The Commission should take note that the problem of unreliable and unregulated public sector endorsements is substantially broader than Amazon Ring alone. EPIC’s ANPR comments focused on endorsements of Amazon Ring by law enforcement organizations because it was the most egregious example of misconduct—however, as noted in EPIC’s ANPR comment, it is not the only example of this kind of unfair and deceptive partnership between a surveillance technology company and a government agency.¹¹ EPIC reiterates here that the Commission should not allow for an exception to its

¹¹ EPIC ANPR Comment at 6, <https://www.regulations.gov/comment/FTC-2022-0070-0043> (“Amazon Ring is by no means the only example of this concerning trend,” citing Flock and Citizen).

important and valuable trade regulation rule for companies who choose government agencies or other non-natural persons to be the mouthpieces for their unsubstantiated claims, especially where the government agency receives compensation that is undisclosed to the consumer. The Commission can mitigate such consumer harm in this rulemaking by being explicit that its rule applies to all companies subject to the Commission's authority, even where the company's chosen endorser may not be subject to the Commission's authority.¹²

To be clear, although the harms inflicted by surveillance technologies frequently outweigh their asserted benefits, EPIC is not urging the Commission to use this rulemaking to directly obstruct government agencies from using such technologies. However, it would be an oversight for the Commission not to hold surveillance technology companies to the same standard as all other companies regarding unsubstantiated claims and undisclosed affiliations which may impact consumer shopping behavior, especially where industry associations have already explicitly voiced concerns about this misconduct.¹³

I. The Commission should explicitly clarify that the definitions in the rule extend to non-natural persons, or else its rule may fail to cover related misconduct.

The following is responsive to Questions 6 and 7.

The Commission's definitions for testimonials proposed under § 465.1(b) and § 465.1(e) should be broadened to explicitly include non-natural persons such as businesses and public sector entities. Offending companies might otherwise argue their endorsers are not covered by the

¹² EPIC ANPR Comment at 11, 13-15.

¹³ EPIC ANPR Comment at 10 (citing to Alfred Ng, *Amazon Ring's Police Partnership 'Troubled' Security Industry Group*, CNET (Aug. 8, 2019), <https://www.cnet.com/news/amazon-rings-police-partnerships-troubled-security-industry-group/>, which quotes The Monitoring Association's President as saying: "[w]e are troubled by recent reports of agreements [between the selling company and law enforcement organizations] that are said to drive product-specific promotion, without alerting consumers about these marketing relationships. This lack of transparency goes against our standards as an industry, diminishes public trust, and takes advantage of these public servants.").

Commission’s rule. The Commission should not limit the efficacy and scope of its rule by remaining silent on this issue.

The proposed language for § 465.1(b) reads:

(b) *Celebrity testimonial* means an advertising or promotional message (including verbal statements, demonstrations, or depictions of the name, signature, likeness, or other identifying personal characteristics of an individual) that consumers are likely to believe reflects the opinions, beliefs, or experiences of a well-known person who purchased, used, or otherwise had experience with a product, service, or business.

The proposed language for § 465.1(e), the definition for "consumer testimonial", is nearly identical, but replaces “well-known person” with “consumer.”

These definitions each describe a message depicting the “name, signature, likeness, or other identifying personal characteristics of an individual” as a testimonial covered by the trade rule.

However, companies publishing or incentivizing violative endorsements could attempt to evade liability by arguing that their endorser was not a natural person and therefore is not covered by the rule. While signature or likeness could arguably apply to a logo or other trademark, and person (“well-known person” in 461.1(b)) could refer to an organization, it seems difficult to argue that “personal characteristics of an individual” would apply to a non-natural person. The Commission should remedy this by clarifying explicitly that its rule applies to non-natural persons. The Commission has already made an analogous clarification for “consumer reviews”,¹⁴ which it explicitly states applies to “purported consumers” (authors who may not actually exist).¹⁵ The Commission should not leave the door open to sellers arguing that the rule does not apply to their misconduct because their endorser is not a natural person and therefore cannot qualify as a “well-known person” or possess “identifying personal characteristics of an individual.”

¹⁴ NPRM at 49,390, <https://www.federalregister.gov/d/2023-15581/p-487>.

¹⁵ NPRM at 49,378, <https://www.federalregister.gov/d/2023-15581/p-302>.

It is important for the Commission to hold sellers chiefly liable for endorsements that violate its rules, even if the Commission can establish liability for the endorser as well. First, an endorser may be undercapitalized or otherwise judgment-proof; the most effective deterrent will be to hold the offending seller company responsible for not adequately overseeing its endorser. In the case of a public sector entity repeating inaccurate or otherwise unsubstantiated claims, the endorser may be beyond the Commission’s jurisdiction entirely—in these instances the only avenue for relief would be to hold the seller responsible for the endorser’s misconduct. Additionally, if the Commission only takes action against the endorsers, that will not incentivize the sellers to change their problematic lack of oversight of their endorsers; as a result, consumers will continue to be harmed by misleading information proliferating in the marketplace as unregulated sellers cycle through unscrupulous endorsers.

Additionally, in EPIC’s ANPR comments, we asked the Commission to consider whether local government entities constituted consumers such that unfair or deceptive practices employed in selling to them would also fall within the purview of the Commission’s trade rule.¹⁶ We are concerned that others will interpret the Commission’s silence on this issue as indicative that local government entities should not be viewed as consumers for the purposes of this trade rule. For similar reasons, the current ambiguity in the proposed rules underscores the need to clarify explicitly that a “consumer” or “celebrity” need not be a natural person, but could include businesses, public sector entities, and other non-natural persons.

¹⁶ EPIC ANPR Comment at 16.

II. The Commission should use a “know or should have known” standard built upon its Endorsement Guides business guidance.

The following is responsive to Questions 8-10.

The knowledge threshold establishes the circumstances under which a company may be liable under the trade rule. A “know or should have known” standard would allow for liability only where the Commission can show that the company actively knew or exercised deficient oversight necessary to discover that its endorsers were violating the rules, whereas a strict liability standard would hold the company responsible for the actions of its endorsers no matter what. EPIC believes the Commission should employ a “know or should have known” standard as to whether the company was aware of a specific endorsement, but it should hold companies strictly liable for unfair or deceptive claims disseminated by their endorsers.

A “know or should have known” standard could draw from the Commission’s Endorsement Guides business guidance, which states that:

It’s unrealistic to expect you to be aware of every single statement made by a member of your network. But it’s up to you to make a reasonable effort to know what participants in your network are saying. That said, it’s unlikely that the activity of one rogue influencer would be the basis of a law enforcement action if your company has a reasonable training, monitoring, and compliance program in place.¹⁷

The lack of an adequate endorser oversight program should be a per se violation of the “know or should have known” standard as it is tantamount to the company deliberately avoiding knowledge.

Additionally, companies should be subject to strict liability for unsubstantiated claims made by their endorsers; to hold otherwise is to undermine the very purpose of the endorsement guides.

The guides state that: “an endorsement may not convey any express or implied representation that would be deceptive if made directly by the advertiser”¹⁸ and that “[a]dvertisers are subject to liability

¹⁷ Fed. Trade Comm’n, *The FTC’s Endorsement Guides: What People Are Asking* (2017), <https://www.ftc.gov/business-guidance/resources/ftcs-endorsement-guides-what-people-are-asking-advertisersresponsibilities>.

¹⁸ *Id.* § 255.1(a).

for misleading or unsubstantiated statements made through endorsements or for failing to disclose unexpected material connections between themselves and their endorsers. An advertiser may be liable for a deceptive endorsement even when the endorser is not liable.”¹⁹ An advertiser or seller should not be able to escape liability for misconduct simply because they paid (or otherwise incentivized) an endorser to put the misrepresentations in the marketplace for them. This is especially important where the endorser does not disclose that they received compensation for their review or testimonial—sellers must exercise adequate oversight to ensure their endorsers disclose to consumers what incentives the seller has made available to them. If sellers are concerned about endorsers creating seller liability, sellers can put measures in place to protect themselves such as indemnification clauses in their contracts with the endorsers.

III. The FTC should take action because surveillance tech vendors regularly use government endorsements to take advantage of consumers.

The following is responsive to Questions 6-10 and Footnote 84.

Amazon Ring is not the only surveillance tech vendor that should be held accountable for statements made by its endorsers.²⁰ And the problem is not limited to police organizations that represent endorsers—healthcare organizations,²¹ including mental health services organizations,²² are being courted by these same surveillance and safety companies including Axon and Amazon.

¹⁹ *Id.* at 255.1(d).

²⁰ The Commission may refer to EPIC’s ANPR comment for several specific examples of how Amazon Ring would be liable under this rule.

²¹ Axon, *The Axon National Healthcare Security Initiative* (<https://www.axon.com/industries/enterprise-security/hospital-security> (2023) (“Under [the 2023 Axon National Healthcare Security] initiative, U.S. hospital security teams are eligible to receive a complimentary Axon Body 3 or up to a \$500 credit on TASER devices per officer when purchasing an Axon Healthcare Security bundle. This initiative also offers a free 60-day trial of Axon’s ecosystem of advanced technology.”).

²² Cyrus Farivar, *Cute videos, But Little Evidence: Police say Amazon Ring Isn’t Much of a Crime Fighter*, NBC News (Feb. 15, 2020), <https://www.nbcnews.com/news/all/cute-videos-little-evidence-police-say-amazon-ring-isn-t-n1136026> (“Senator Markey’s office maintains that Amazon Ring is actively recruiting public health departments, animal services, and agencies that primarily address homelessness, drug addiction, and mental health, despite Amazon Ring stating that only police and fire departments are currently on its platform”).

The proposed rules might exclude these organizations, leaving consumers unprotected from particularly influential misleading endorsements, and exposing government agencies themselves to misleading and deceptive marketing.

Under existing rules, a seller must substantiate its explicit efficacy claims and its implicit accuracy claims before its endorsers can disseminate those claims.²³ This includes claims about crime reduction, which imply a consumer utilizing the surveillance technology can expect a reduction in crime in their neighborhood or against their person. Additionally, a seller must ensure its endorsers disclose any affiliate relationship to the consumer²⁴—including compensation received in the form of discounted products and of access to a user’s data without first obtaining that user’s consent.

The endorsement guides state that “[a]n advertiser may be liable for a deceptive endorsement even when the endorser is not liable.”²⁵ However, the Commission’s proposed trade rule does not include a similar statement. EPIC does not urge the Commission to use this rulemaking to stop government agencies from purchasing technology from vendors; rather, we ask that the Commission consistently enforce its rules concerning endorsements so that surveillance tech companies do not enjoy an unfair market advantage when they engage public sector agencies and other entities as their endorsers.

²³ FTC, *Policy Statement Regarding Advertising Substantiation* (Nov. 23, 1984), <https://www.ftc.gov/legal-library/browse/ftc-policy-statement-regarding-advertising-substantiation>; FTC, *Advertising Substantiation Principles Training Guide* (undated), <https://www.ftc.gov/sites/default/files/attachments/training-materials/substantiation.pdf>; FTC, *Notice of Offenses Concerning Substantiation of Product Claims* (Apr. 13, 2023), <https://www.ftc.gov/enforcement/notices-penalty-offenses/penalty-offenses-concerning-substantiation>.

²⁴ FTC, *FTC’s Endorsement Guides: What People Are Asking* (Jun. 2023), <https://www.ftc.gov/business-guidance/resources/ftcs-endorsement-guides-what-people-are-asking#affiliateornetwork>; FTC, *Disclosures 101 for Social Media Influencers* (Nov. 2019), <https://www.ftc.gov/business-guidance/resources/disclosures-101-social-media-influencers>.

²⁵ FTC Endorsement Guides § 255.1(d).

Companies often make efficacy and accuracy claims that are unsubstantiated (and sometimes even directly contradicted by evidence from other police departments). Police endorsements can boost consumer sales, especially with respect to personal safety products. For example, the founders of Taser relied heavily on police endorsements because they “believed that the Taser would always be perceived as a silly gadget unless, like the Maglite, it was endorsed by law enforcement.”²⁶ Endorsements from public sector agencies carry significant weight with the public, making them highly valuable for corporations.

Non-natural persons such as police departments regularly endorse products both explicitly (for example, through promotional material promoting their use) and implicitly (for example, through entering partnerships with companies like Noonlight and accepting donations from companies affiliated with manufacturers like Taser).²⁷ This can include the seller company writing press releases to be posted by police departments and police providing the company with neighborhood contact lists (e.g., Flock Safety’s promotional practices).²⁸ Public sector endorsements are especially problematic when the agency fails to disclose a relationship with the vendor (like

²⁶ Dana Goodyear, *Can the Manufacturer of Taser Provide the Answer to Police Abuse*, The Verge (Aug. 20, 2018), <https://www.newyorker.com/magazine/2018/08/27/can-the-manufacturer-of-tasers-provide-the-answer-to-police-abuse>.

²⁷ Kevin Johnson, *Police group receives donation from Taser stun-gun maker*, USA Today (Oct. 21, 2012), <https://www.usatoday.com/story/news/nation/2012/10/21/taser-police-chiefs/1627299/> (“‘When you accept that kind of donation, you create an impression that you view the product favorably,’ said the executive director of the nation’s largest police union in response to the International Association of Chiefs of Police Foundation accepting a donation from the foundation associated with Taser International.”)

²⁸ *Id.* at 3 (“Flock has also helped write police press releases, Vice found, and officers appear in Flock promotional videos. Emails obtained by the video surveillance industry research group IPVM show local Texas police referring homeowners associations and other neighborhood groups to Flock, advocating for the company at community meetings, providing the company with neighborhood contact lists, and introducing other police chiefs to company sales managers.”).

surveillance tech vendor Vigilant solutions)²⁹ or fails to disclose other problematic practices by the vendor (like Life360).³⁰

Here we highlight several prominent companies that use public sector entities to market their products and make efficacy claims without substantiation. The throughline of Flock Safety, Axon, and Noonlight is that public sector agencies benefit from free data and normalization of advanced surveillance in policing practices, while the companies can make sales to the public endorsed by trusted public entities.

a. Flock Safety and law enforcement partners claim that license plate readers cause extraordinary reductions in crime.

Flock Safety sells license plate reader camera systems for both police and civilian use. Flock’s license plate readers and associated software systems are regularly used by private neighborhoods and individuals. For instance, Flock markets a webinar for landlords and retail property owners on “Proactively Preventing and Solving Crime at Your Properties” claiming that Flock cameras can accomplish substantial decreases in crime.³¹ The video features David Ballard, a former police lieutenant who left the public sector to work for Flock, claiming that a 34 percent decrease in crime in Memphis, TN was due to Flock Safety.³² The video also claims that 7 percent of

²⁹ Jonathan Bullington, Kala Kachmar, & Mike Trautmann, *What you should know about those license plate readers popping up in neighborhoods*, Louisville Courier Journal (Apr. 11, 2022), <https://www.courier-journal.com/story/news/crime/2022/04/11/license-plate-readers-do-they-work-as-claimed-stop-crime/9536177002/> (“In 2016, three police departments in Texas developed agreements with a tech company, Vigilant Solutions, which is now Motorola Solutions, that supplied free license plate readers and credit card machines for departments to keep in police vehicles. In exchange, the company received a 25% surcharge on the court fines for outstanding warrants or violations processed upon being pulled over — essentially giving motorists a choice to pay or go to jail.”).

³⁰ Jon Keegan & Alfred Ng, *Following Markup Investigation, U.S. Regulators Questioned Life360’s Data Practices*, The Markup (Apr. 1, 2022), <https://themarkup.org/privacy/2022/04/01/following-markup-investigation-u-s-regulators-questioned-life360s-data-practices>.

³¹ Flock Safety, *Webinar: Proactively Preventing and Solving Crime at Your Properties* (Sept. 14, 2023), <https://www.flocksafety.com/resources/preventing-crime-at-your-properties>.

³² *Id.* In the webinar, Ballard also claims that 7 percent of crimes in the U.S. are solved with Flock Safety’s technologies and makes a series of misleading statements accounting for crime solved as crimes prevented. *See id.*

crimes in the United States are solved using Flock’s LPR cameras and software.³³ Flock has also had law enforcement partners regularly make claims about Flock cameras driving substantial crime reductions based on short-term, unscientific studies.³⁴ For example, Flock promotes a video and associated blog post claiming a 70% reduction in crime in San Marino, California between May 2020 and May 2021.³⁵

But the evidence just isn’t there that license plate readers prevent crime. Year-over-year comparisons in crime rates are notoriously unreliable as measures of any policy effectiveness,³⁶ and the best studies suggest that license plate reader have little if any effect on preventing or reducing crime.³⁷ In one industry-wide study, approximately 10% of license plates were misidentified by license plate readers, an alarming error rate which can lead to the arrest of innocent people.³⁸

Yet Flock continues to rely on law enforcement assertions of crime reduction in both company materials and ostensibly independent endorsements. In fact, Flock “works closely with

³³ *Id.*

³⁴ Hope Ford, *Police say license plate readers help reduce crime. But, how is the data being used?*, 11alive (Oct. 22, 2019), <https://www.11alive.com/article/news/crime/cobb-county-crime-reduces-thanks-to-flock-cameras-license-plate-readers/85-c0b70476-6adf-447c-901c-d560288f2cfd> (“Cobb County Police said new technology is helping them stop and catch criminals with a simple camera attached to a pole. ‘It’s been eye-opening. Nobody expected this drop,’ said Deputy Chief Stuart VanHoozer.”).

³⁵ Flock Safety, *How Technology Can Help Reduce Gun Violence* (Jul. 29, 2021), <https://www.flocksafety.com/articles/alpr-technology-gun-violence>.

³⁶ See e.g., Keshia S. Moore, Ryan Tom, & Jackie O’Neill, *The Truth Behind Crime Statistics: Avoiding Distortions and Improving Public Safety*, Thurgood Marshall Institute (Aug. 3, 2022), <https://www.naacpldf.org/wp-content/uploads/2022-08-03-TMI-Truth-in-Crime-Statistics-Report-FINAL-2.pdf>.

³⁷ Jonathan Hofer, *Oakland’s Automated License Plate Reader (ALPR) Debacle*, Catalyst (Aug. 16, 2023), <https://catalyst.independent.org/2023/08/16/oaklands-automated-license-plate-reader-alpr/>.

³⁸ Jay Stanley, *Fast-Growing Company Flock is Building a New AI-Driven Mass-Surveillance System*, ACLU at 5 (Mar. 3, 2022), <https://www.aclu.org/report/fast-growing-company-flock-building-new-ai-driven-mass-surveillance-system> (“In particular, IPVM found that Flock’s system misidentified a license plate’s state about 10 percent of the time. Given that state misidentification errors have led to innocent people being terrorized by the police as presumed dangerous criminals, that is a real problem.”).

police to try and generate positive media coverage, improve their PR strategy, and . . . ‘bring more private cameras into the area.’”³⁹

b. Axon (formerly Taser) uses police endorsements to support debunked claims that its products for personal and police use are “non-lethal.”

Axon has for years relied on police endorsements of the safety and efficacy of its technologies. While many Axon products are designed for police use,⁴⁰ the company offers several civilian versions of its Taser stun guns, including a “Professional Series” of stun guns for the general public.⁴¹ Despite years of reporting and well over 1,000 recorded deaths from Taser weapons, the company continues to market some of its stun gun products as a “non-lethal defense tool.”⁴² As Reuters documented in depth, Axon marketed its products for years as non-lethal and with no lasting health risks.⁴³ These same claims, which were based on shoddy science and repeated regularly by Axon’s CEO, appear in promotions by police officers. In one prominent example from 2003, a police officer pitched Taser products to his local city council without disclosing that he had been paid by Axon in stock options.⁴⁴ Police officers continue to promote Tasers as “non-lethal” weapons to this day.⁴⁵ Axon is another example of a company that makes false or misleading claims about

³⁹ Joseph Cox, *Inside ‘TALON,’ the Nationwide Network of AI-Enabled Surveillance Cameras*, Vice News (Mar. 3, 2021), <https://www.vice.com/en/article/bvx4bq/talon-flock-safety-cameras-police-license-plate-reader>.

⁴⁰ Axon, *Law Enforcement Product Catalog* (2023), <https://www.axon.com/products?productCategory=cews>.

⁴¹ Axon, *Taser Product Catalog, Professional Series Taser 7 CQ* (2023), <https://taser.com/pages/professional-series>.

⁴² *Shock Tactics: inside Taser, the weapon that transformed policing*, Reuters Investigates (2017), <https://www.reuters.com/investigates/section/usa-taser/>; Axon, *Taser Product Catalog, Taser Pulse* (2023), <https://taser.com/pages/all-devices> (“TASER Pulse is an effective, non-lethal defense tool that can immobilize attackers for up to 30 seconds.”).

⁴³ Lisa Girion, *The garage science behind the stun gun that changed policing*, Reuters (Sept. 20, 2017), <https://www.reuters.com/investigates/special-report/usa-taser-science/>.

⁴⁴ *Stun Gun Fallacy, How the Lack of Taser Regulation Endangers Lives*, ACLU at 7 (Sept. 2005), <https://www.aclunc.org/sites/default/files/Stun%20Gun%20Fallacy%20-%20How%20the%20Lack%20of%20Taser%20Regulation%20Endangers%20Lives.pdf>.

⁴⁵ See, e.g., Dave Askins, *Tasers for Bloomington police: Department prepares for pilot program on less lethal weapon*, B Square Bulletin (Sept. 23, 2023), <https://bsquarebulletin.com/2023/09/23/tasers-for-bloomington-police-department-prepares-for-pilot-program-on-less-lethal-tool/> (“Responding to a question

products sold to both police and civilians and relies on law enforcement endorsements of safety and effectiveness to market their products.

c. Noonlight (formerly SafeTrek) keeps close relationships with police and metropolitan transit agencies.

Noonlight is a company selling smart device-connected apps for personal safety, car crash monitoring, and home monitoring that can automatically contact police and send audio and video footage to them. Noonlight also offers data analysis for police departments with hot-spot mapping, trend-monitoring, and response-analysis.⁴⁶ Noonlight claims a 1 percent false alarm rate for calls to police through the app, although the data behind that number has not been made public.⁴⁷ The company leveraged local connection to receive endorsements from multiple St. Louis, MI governmental or quasi-governmental agencies, including the St. Louis Downtown Community Improvement District and transit authority.⁴⁸ Noonlight also offered free subscriptions in partnership with the St. Louis Metropolitan Transit Authority.⁴⁹ This type of close corporate relationship with local governments warrants scrutiny to ensure that false or misleading information is not broadcast by government agencies.

But Noonlight’s effectiveness claims were often overstated. When a news outlet tested Noonlight’s GPS accuracy and police response times, it found that the app was not providing

from The B Square last week, Jeff Rodgers, who is one of the police union representatives, said that issuing tasers to the Bloomington police officers would not help recruitment efforts, ‘because it is an industry standard in law enforcement.’ Rodgers continued, ‘Almost every other department in the nation already carries tasers as a part of their non-lethal equipment.’”).

⁴⁶ Noonlight, *Public Safety* (2023), <https://www.noonlight.com/public-safety>.

⁴⁷ *Id.*

⁴⁸ Downtown St. Louis Community Improvement District, *A Safer Downtown District* (2023), <https://www.stlclid.org/safer>, (“We recommend the Noonlight (formerly SafeTrek) app, which has a free version and is available for both iOS and Android.”).

⁴⁹ *St. Louis Metro extends partnership with safety app*, *Noonlight*, Metro Magazine (Apr. 23, 2019), <https://www.metro-magazine.com/10031517/st-louis-metro-extends-partnership-with-safety-app-noonlight>.

accurate GPS location and took substantially longer to contact police than a simple phone call.⁵⁰ At times, Noonlight also appears to have overstated its relationship with police departments. In 2017, Noonlight was used heavily on college campuses in Philadelphia, but neither Philadelphia police nor the campus police department were familiar with the app.⁵¹

The company website prominently features endorsements from police and first responders speaking in their professional capacity:

There are a lot of situations where someone could be in some form of danger and not have a split second to dial 911, or could have a medical emergency where they were physically unable to talk. We don't usually push for businesses, but this product proved too good to pass up.- SGT. Chris Malek, River Hills Police Department.⁵²

IV. Conclusion

We thank the Commission for the opportunity to comment on this rule and urge that the Commission both ensure that consumers are protected from deceptive endorsements regardless of what entity publishes them and safeguard competition by holding all sellers accountable to the same rules, regardless of what entities they select as endorsers.

Respectfully submitted,

/s/ John Davisson
John Davisson
Director of Litigation

/s/ Jake Wiener
Jake Wiener
Counsel

/s/ Chris Frascella
Chris Frascella
Counsel

⁵⁰ CBS, *Testing Popular Safety App Noonlight's Response Time Compared To 911*, CBS Philadelphia (Nov. 26, 2019), <https://www.cbsnews.com/philadelphia/news/testing-popular-safety-app-noonlights-response-time-compared-to-911/>.

⁵¹ Michaela Winberg, *Why Philly police are skeptical of this safety app that alerts 911*, WHYY Billy Penn (Jun. 30, 2017), <https://billypenn.com/2017/06/30/why-philly-police-are-skeptical-of-this-safety-app-that-alerts-911/>.

⁵² Noonlight, *Public Safety* (2023), <https://www.noonlight.com/public-safety/>.