Amazon Ring Master of the Surveillance Circus

Christopher Frascella*

TABLE OF CONTENTS

* J.D., May 2021, The George Washington University Law School. Thank you to Matthew Guariglia, Nat Meysenburg, and Prof. Andrew Ferguson for taking the time to offer seasoned perspective on the lack of oversight of surveillance technologies. Major thanks to my colleagues in the Federal Communications Law Journal, in particular for their promptness and patience with incorporating news updates as practices evolved, but also more generally for their collegial support and diligent attention throughout the review process.

I. INTRODUCTION

In an era when many call for defunding police departments and when racial inequities in policing and surveillance are at the fore, it is important for local law enforcement to cultivate trust with the people they protect by improving the transparency and accountability of their surveillance practices. Instead, hundreds of departments are operating like marketing partners, and in at least one instance facilitating and subsidizing the sale of one company's surveillance tech products to consumers.

This Note will focus on police departments' promotion of Amazon Ring doorbell cameras—surveillance tech that, by design, enables police to request access to footage from consumers before requesting a warrant from courts—and of the related Neighbors app, which combines aspects of a neighborhood watch program and an online message board, and allows for easy sharing of Ring footage.[1] Police departments have received compensation from Amazon for their efforts in the form of discounted Amazon Ring units proportionate to the number of local downloads of Amazon's Neighbors app, promoted Amazon products openly over their official social media accounts, and signed agreements giving Amazon oversight over police departments' public communications about Amazon's products.[2]

Surveillance technology companies should be held to the same standard of transparency and truthfulness in advertising as other industries. Similarly, police departments should be treated as any other marketing organization when acting as influencers. Consumer protection law can be used to compel disclosure of these relationships, and to create the resistance that should exist when police departments become complicit in peddling a nationwide surveillance network of questionable efficacy and demonstrated capacity to exacerbate existing social inequities.

Communities can now aggregate information and act with greater speed and ease than ever before—including facilitating the deployment of law enforcement resources. By virtue of American privacy law's slow development and Amazon's clever strategy in incentivizing law enforcement to market its products, Amazon Ring created a network of doorbell surveillance cameras potentially accessible to police departments by a single click rather than by a warrant. While this is a threat to the privacy of any individual who happens to be "in frame" of one or more doorbell cameras, partnerships like these pose additional risk to communities of color due to the social, technological, and institutionalized racial biases at play. This systemic threat is growing at breakneck speed, in large part because Amazon has deputized local police as a partner marketing channel.

Consumer protection law may provide the only immediate friction to slow this otherwise rapid and geographically widespread deterioration of civil

1. *See The Ring Story*, RING, https://ring.com/about (last visited Jan. 27, 2021) [https://perma.cc/B4H2-M9MA].

2. *Infra* Section II.

liberties by forcing transparency regarding the nature of the relationships between local police departments and Amazon Ring. This Note begins in Section II with an overview of relevant Amazon products, Ring and Neighbors, and an overview of why without enacted federal privacy legislation, consumer protection law may be the only remedy immediately available. Section III provides context as to the growth of surveillance technology and the relationship between surveillance tech vendors and police departments. A more detailed explanation follows in Section IV of why traditional legal remedies do not apply to situations like that of Amazon Ring and why that legal impotence is unlikely to change soon. This Note concludes with a brief analysis of (1) state Unfair and Deceptive Acts or Practices (UDAP) laws and (2) the FTC's Endorsement Guides, explaining how they serve as the best means for immediate redress.

II. SURVEILLANCE, STARTUP CULTURE, AND SOCIETY

A. Ring is Intuitively Troubling, But Permissible

Despite the threats to the privacy of consumers and non-consumers, there are no legal barriers to use of the Ring product. Homeowners choose to purchase a Ring doorbell camera unit, sign a contract giving Amazon ownership of the data, install the Ring unit appropriately (so that it captures video of their doorstep), and provide the required consent (often by clicking a button in an automated email)[3] for the police to access the Ring video feed.

Because of this structure, Ring customers are not compelled to do anything with their property. Amazon is not responsible for customer misuse. Police cannot access the video without either the property owner's permission or a warrant.[4] And passers-by captured on video have no expectation of privacy while walking in public view.

Moreover, Amazon ceased two of its most questionable practices: providing police departments with (1) heat maps of Ring coverage and (2) reports of property owners who deny their local department's requests to view their Ring data. As of 2020, Amazon allows users to preemptively opt out of requests from police to the user, and as of 2021, offers opt-in encryption to

3. Drew Harwell (@drewharwell), TWITTER (Aug. 28, 2019, 1:55 PM), https://twitter.com/drewharwell/status/1166771255724453890.

4. *See Ring Law Enforcement Guidelines*, RING, https://support.ring.com/hc/en-us/articles/360001318523-Ring-Law-Enforcement-Guidelines (last visited Feb. 2, 2021) [https://perma.cc/3SWD-BL8B] ("Ring distinguishes between content and non-content information. We may produce non-content information in response to a valid subpoena, search warrant, or other court order. Content information will only be disclosed in response to a valid search warrant or with the consent of the account owner."); *see generally Law Enforcement Information Requests in 2020*, RING, (last visited April 19, 2021) https://blog.ring.com/2021/01/20/law-enforcement-information-requests-in-2020/ (providing a report on the company's responses to law enforcement requests during 2020).

ensure Ring data is not visible without deliberate action from the user.[5] Arguably, Ring is exhibiting the 21st century "move fast and break things" startup culture in rolling out a new product.[6]

As for other obvious stakeholders, property owners have the right to protect their property interests, and police are within their rights to fulfill their public safety mandate using the most efficient means available, assuming those means are legal.

B. Today's Privacy Harms, Made Worse Tomorrow

Consumers who purchase Ring equipment and do not opt-in to encryption are subject to Amazon harvesting and using their data. However, arguably the greater risk here is to those who do not purchase the equipment but are still surveilled. As the use of Ring grows, communities will be subject to constant surveillance, with questionable accuracy and limited accountability.[7] This becomes truly chilling when combined with experimental technologies already gaining traction in the marketplace, such as facial recognition (FR), which promises to create a 21st century corporate panopticon.[8] Admittedly, Amazon has implemented a self-imposed

5. Ring, *The New Control Center Empowers Ring Customers to Manage Important Privacy and Security Settings*, RING BLOG (Jan. 30, 2020), https://blog.ring.com/2020/01/30/the-new-control-center-empowers-ring-customers-to-manage-important-privacy-and-security-settings/ [https://perma.cc/YJ7S-T3MT]; Ring, *Understanding Video End-to-End Encryption (E2EE),* RING SUPPORT, https://support.ring.com/hc/en-us/articles/360054941511-Understanding-Video-End-to-End-Encryption-E2EE- (last accessed Feb. 20, 2021).

6. *See generally* Hemant Taneja, *The Era of "Move Fast and Break Things" is Over*, HARV. BUS. REV. (Jan. 22, 2019), https://hbr.org/2019/01/the-era-of-move-fast-and-break-things-is-over [https://perma.cc/3SAW-T249].

7. Advocates concerned about the military-industrial complex-esque expansion of police power via deep discount Big Tech surveillance would certainly prefer to win this kind of fight on privacy grounds. However, the unfortunate fact is that the vast majority of Americans are without the legal authority to prevail in defending their privacy against corporations collecting and/or selling their behavior (and now their neighbors' behavior) as a digital commodity. Europe recently revoked the United States' special status for data transfers due to the extent of disproportionately extensive government surveillance and the lack of remedy for those subject to it. Court of Justice of the European Union, *The Court of Justice Invalidates Decision 2016/1250 On The Adequacy Of The Protection Provided By The EU-US Data Protection Shield*, Press Release No 91/20, CURIA (July 16, 2020), https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf [https://perma.cc/54MD-9T5Q]. Understandably, this massive collection of data by law enforcement agencies has implications for those concerned with criminal justice reform. *See, e.g.*, ANDREW GUTHRIE FERGUSON, THE RISE OF BIG DATA POLICING: SURVEILLANCE, RACE, AND THE FUTURE OF LAW ENFORCEMENT (2019).

8. "Through this seemingly constant surveillance, Bentham believed all groups of society could be altered." *Ethics Explainer: The Panopticon*, ETHICS CTR. (Jul. 18, 2017), https://ethics.org.au/ethics-explainer-panopticon-what-is-the-panopticon-effect/.

moratorium on selling facial recognition technology to law enforcement.[9] However, this does not address the underlying surveillance technology infrastructure problem, especially if in selling these products to consumers, Amazon facilitates sharing that data with police departments, as part of the product's design.[10] These in-roads to a surveillance state are forming faster than the public's ability to understand and respond to the threats they pose; this is in large part because police often endorse solutions, such as Ring and the related Neighbors app, from the Amazon surveillance suite.[11]

Discussion of the Neighbors app below illustrates how this kind of surveillance can harm the fabric of a community, often with racist subtext. One Amazon worker argued that Ring is "not compatible with a free society."[12] An Amazon software engineer offered: "The privacy issues are not fixable with regulation, and there is no balance that can be struck. . . . Ring should be shut down immediately and not brought back."[13]

In terms of criminal justice implications, Supreme Court case law suggests that errors made as a result of imperfect database-driven technologies, which can easily result in wrongful identifications (perhaps even of members of Congress[14]), could be excused by the "good-faith" rule,[15] meaning American citizens have no reasonable expectation of accountability

---

9. Isobel Asher Hamilton, *Outrage Over Police Brutality Has Finally Convinced Amazon, Microsoft, and IBM to Rule Out Selling Facial Recognition Tech to Law Enforcement. Here's What's Going on*, BUS. INSIDER (June 13, 2020), https://www.businessinsider.com/amazon-microsoft-ibm-halt-selling-facial-recognition-to-police-2020-6?op=1 [https://perma.cc/F65P-2RU5].

10. Namely, it does not preclude further development of the infrastructure upon which FR can be readily deployed once companies' moratoria end. *See* Caroline Haskins, *Amazon, IBM, And Microsoft Won't Say Which Police Departments Used Their Facial Recognition Technology*, BUZZFEED NEWS (June 12, 2020), https://www.buzzfeednews.com/article/carolinehaskins1/amazon-ibm-and-microsoft-wont-say-which-police-departments [https://perma.cc/8V2X-E3A3].

11. *See generally Neighbors by Ring*, RING, https://ring.com/neighbors (last visited Oct. 21, 2020) [https://perma.cc/BP63-LBUY]. Neighbors is a social media platform that combines aspects of neighborhood watch and a community bulletin board. Another example of this kind of product is Nextdoor. Chris Taylor, *Nextdoor Is Next: Why the Social Network of Systemic Racism Is Ripe for Change*, MASHABLE (June 11, 2020), https://mashable.com/article/nextdoor-racism/ [https://perma.cc/Q336-GTMB]. Amazon's suite of tools includes the controversial Sidewalk project as well. Ry Crist, *Amazon Sidewalk Will Create Entire Smart Neighborhoods. Here's What You Should Know*, CNET (Oct. 7, 2020), https://www.cnet.com/how-to/amazon-sidewalk-will-create-entire-smart-neighborhoods-faq-ble-900-mhz/ [https://perma.cc/H7XU-FDBK].

12. Jay Greene, *Amazon Employees Launch Mass Defiance of Company Communications Policy in Support of Colleagues*, WASH. POST (Jan. 27, 2020), https://www.washingtonpost.com/technology/2020/01/26/amazon-employees-plan-mass-defiance-company-communications-policy-support-colleagues/ [https://perma.cc/N8DY-EU8X].

13. *Id.*

14. *See* Russell Brandom, *Amazon's Facial Recognition Matched 28 Members of Congress to Criminal Mugshots*, VERGE (Jul. 26, 2018) https://www.theverge.com/2018/7/26/17615634/amazon-rekognition-aclu-mug-shot-congress-facial-recognition.

15. *See* Herring v. United States, 555 U.S. 135, 142–44 (2009) (finding negligently maintained database did not amount to systemic error).

for police or for vendors of hastily deployed, FR-amplified surveillance tech, except perhaps in the most egregious of circumstances. And we can expect such errors will occur, indeed, some already have.[16] A recent study by the National Institute of Standards and Technology (NIST) documented the potential extent of race-based disparities in the accuracy of the technology: Asian and African American people were up to 100 times more likely to be misidentified by this technology than white men, with Native American subjects experiencing the highest rate of false positives.[17]

The technological infrastructure is already in place. Amazon has attempted to sell its own FR product called Rekognition [18] to police departments[19] and already filed a patent to use FR technology in conjunction with Ring.[20] As of late 2019, there were more than 7 million downloads of the companion app, Neighbors.[21] Globally, more than 10 million Ring units have been installed.[22] And by the end of 2020, forty-eight states had at least one police or fire department participating in the Ring program, with local

16. Although not a result of Amazon Ring, there are already three documented cases of false arrests caused by improper use of FR technology. *See, e.g.*, Bobby Allyn, *'The Computer Got It Wrong': How Facial Recognition Led to False Arrest of Black Man*, NPR (June 24, 2020), https://www.npr.org/2020/06/24/882683463/the-computer-got-it-wrong-how-facial-recognition-led-to-a-false-arrest-in-michig [https://perma.cc/3JZX-DFE4]; Kris Holt, *Facial Recognition Linked to A Second Wrongful Arrest by Detroit Police*, ENGADGET (July 10, 2020), https://www.engadget.com/facial-recognition-false-match-wrongful-arrest-224053761.html [https://perma.cc/KXT3-5BEX]; Kashmir Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*, N.Y. TIMES (Dec. 29, 2020, updated Jan. 6, 2021), https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html.

17. Drew Harwell, *Federal Study Confirms Racial Bias of Many Facial-Recognition Systems, Casts Doubt on Their Expanding Use*, WASH. POST (Dec. 19, 2019), https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/ (Amazon opted not to participate in NIST's study, though 99 other companies, academic institutions, and developers did) [https://perma.cc/JQW4-RV25].

18. *See geneally What Is Amazon Rekognition?*, AMAZON WEB SERVS., https://docs.aws.amazon.com/rekognition/latest/dg/what-is.html (last visited Apr. 14, 2020) [https://perma.cc/YX9Y-XZ47].

19. An Amazon Employee, *I'm an Amazon Employee. My Company Shouldn't Sell Facial Recognition Tech to Police*, MEDIUM (Oct. 16, 2018), https://medium.com/@amazon_employee/im-an-amazon-employee-my-company-shouldn-t-sell-facial-recognition-tech-to-police-36b5fde934ac [https://perma.cc/VRV2-ZWBX].

20. U.S. Patent Application No. US 2018/0341835 A1 (filed Nov. 29, 2018) https://www.aclunc.org/docs/Amazon_Patent.pdf (last accessed Apr. 14, 2020) [https://perma.cc/C5N3-FSGK]. However, Amazon announced an undefined "moratorium" on law enforcement use of Amazon's facial recognition technology until June 2021. Alfred Ng, *Amazon Owes Answers On Facial Recognition Moratorium, Lawmaker Says*, CNET (June 17, 2020), https://www.cnet.com/news/amazon-owes-answers-on-facial-recognition-moratorium-lawmaker-says/ [https://perma.cc/CH4Y-SVNA].

21. Sarah Perez, *Amazon's Ring Partners With National Center for Missing & Exploited Children to Put Missing Posters in Neighbors App*, TECHCRUNCH (Dec. 19, 2019), https://techcrunch.com/2019/12/19/amazons-ring-partners-with-national-center-for-missing-exploited-children-to-put-missing-posters-in-neighbors-app/ [https://perma.cc/LDF2-EVCC].

22. *Id.*

law enforcement agencies in at least two states piloting programs to integrate Ring footage into their Real Time Crime Centers.[23]

C. A Solution to Protect Consumers and Non-Consumers

There have been several local bans[24] and attempts at federal legislation[25] to address privacy concerns of facial recognition specifically. But national security expert Bruce Schneier aptly argues that focusing on facial recognition misses the bigger point:

> A ban on facial recognition won't make any difference if, in response, surveillance systems switch to identifying people by smartphone MAC addresses. The problem is that we are being identified without our knowledge or consent, and society needs rules about when that is permissible.[26]

Schneier goes on to argue for consumer protection-style solutions, including regulation of data brokers and additional consumer education and debate: "We need to have a serious conversation about all the technologies of identification, correlation and discrimination, and decide how much we as a

---

23. Kim Lyons, *Amazon's Ring Now Reportedly Partners with More Than 2,000 US Police and Fire Departments*, VERGE (Jan. 31, 2021), https://www.theverge.com/2021/1/31/22258856/amazon-ring-partners-police-fire-security-privacy-cameras [https://perma.cc/4WEH-S3ZB] (noting participating police and fire departments rose from 40 in 2018 to 2,014 in 2020); Matthew Guariglia, *Police in Mississippi to Pilot a Program to Live-Stream Amazon Ring Cameras*, MOZILLA FOUND. (Nov. 19, 2020), https://foundation.mozilla.org/en/blog/police-mississippi-pilot-program-live-stream-amazon-ring-cameras/ [https://perma.cc/UXD8-ZBME] (including Amazon's response, distancing itself from Jackson program); *see Surveillance Compounded: Real-Time Crime Centers in the U.S.*, ATLAS SURVEILLANCE, https://atlasofsurveillance.org/real-time-crime-centers (last visited Nov. 21, 2020) (noting that Leon County, FL implemented a similar program integrating Ring data into its Real Time Crime Centers) [https://perma.cc/7M25-JKCT].

24. *San Francisco Bans Facial Recognition*, EPIC (May 15, 2019), https://epic.org/2019/05/san-francisco-bans-facial-reco.html [https://perma.cc/4H82-MU7Q]; *e.g.*, *Ban Facial Recognition*, https://www.banfacialrecognition.com/map/ (last visited Oct. 21, 2020) (showing restrictions in California, Massachusetts, Mississippi, Maine, and Oregon via an interactive map) [https://perma.cc/E2P8-QNMY]; Eric Einhorn, *A Fight Over Facial Recognition Is Dividing Detroit - With High Stakes for Police and Privacy*, NBC NEWS (Aug. 22, 2019), https://www.nbcnews.com/news/us-news/fight-over-facial-recognition-dividing-detroit-high-stakes-police-privacy-n1045046 (indicating that Detroit is likely to restrict law enforcement use of the technology) [https://perma.cc/ZLU6-BHCA].

25. *See, e.g.*, *Grading on a Curve: Privacy Legislation in the 116th Congress (2019-2020)–Updated*, ELEC. PRIV. INFO. CTR. (Apr. 2020), https://epic.org/GradingOnACurve/EPIC-GradingOnACurve-Apr2020.pdf [https://perma.cc/6BHL-BNTH]; *Senators Demand Information From Amazon on Ring and Surveillance*, EPIC (Nov. 21, 2019), https://epic.org/2019/11/senators-demand-information-fr.html [https://perma.cc/CSP7-GW3S].

26. Bruce Schneier, *We're Banning Facial Recognition. We're Missing the Point.*, N.Y. TIMES (Jan. 20, 2020), https://www.nytimes.com/2020/01/20/opinion/facial-recognition-ban-privacy.html [https://perma.cc/WAV5-BTKT].

society want to be spied on by governments and corporations—and what sorts of influence we want them to have over our lives."[27]

In short: Do the risks associated with using the technology outweigh the risks associated with not using it? While American society grapples with that deeper question, the legal community can answer two additional, but much narrower and simpler questions:

1) What does it look like to hold surveillance technology companies to the same standards as other industries regarding the transparency of their sales practices and the truthful advertising surrounding the effectiveness of their products?
2) How can the law ensure that recruiting police departments as social media influencers does not allow those companies to bypass those standards?

Much can be said about this "perfect storm of privacy threats"[28] and the problem of partnerships between global surveillance-based technology companies and local law enforcement.[29] This Note will address only the what, the why, the who, and the how of using consumer protection law to compel disclosure of the relationship between police departments and companies selling products like Amazon Ring. There should be a natural friction when Big Tech sells surveillance equipment nationwide to facilitate behavioral data collection in the guise of promoting public safety—but these partnerships with police have reduced that friction.

Consumer protection law can provide a model to address the privacy threats posed by corporate partnerships with law enforcement, like police endorsements and sales of Amazon Ring—by attaching penalties to a lack of transparency in these partnerships as they would with any other form of misleading advertising. These partnerships should be fully disclosed to consumers in promotional materials, as any other marketing relationship

27. *Id.*

28. Matthew Guariglia, *Amazon's Ring Is a Perfect Storm of Privacy Threats*, ELEC. FRONTIER FOUND. (Aug. 8, 2019), https://www.eff.org/deeplinks/2019/08/amazons-ring-perfect-storm-privacy-threats [https://perma.cc/JSB4-NRLZ].

29. *See* Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. TIMES (Jan. 18, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html [https://perma.cc/C3Y8-XRAS]. There are many examples of agreements between police departments and surveillance technology vendors, secret even from police leadership. *See, e.g.*, Tim Cushing, *Harris Stingray Nondisclosure Agreement Forbids Cops From Telling Legislators About Surveillance Tech*, TECHDIRT (Jan. 25, 2018), https://www.techdirt.com/articles/20180120/06352239048/harris-stingray-nondisclosure-agreement-forbids-cops-telling-legislators-about-surveillance-tech.shtml [https://perma.cc/L8PV-5FKJ]; Alex Boutilier, et al., *Clearview AI to Pull Out of Canada and Stop Working with RCMP Amid Privacy Investigation*, THE STAR (July 6, 2020), ("More than a dozen police services initially told the Star their forces hadn't tested the tool only to later confirm that officers had used trial versions of Clearview AI without the knowledge or authorization of police leadership.") https://www.thestar.com/news/canada/2020/07/06/clearview-ai-to-pull-out-of-canada-and-stop-working-with-rcmp-amid-privacy-investigation.html [https://perma.cc/2A6V-2E5C].

would be. This still offers no direct redress for bystanders captured by this technology, but it does create greater opportunity for public debate about private-public surveillance partnerships, which could indirectly mitigate the impact of second order privacy harms.

In fact, until a meaningful federal privacy law is passed, consumer protection law is the best, and perhaps only, immediate legal solution to combat the alarming growth of these corporate-law enforcement surveillance partnerships and to increase transparency among consumers and concerned citizens.

III. AMERICA'S SURVEILLANCE ZEITGEIST

A. Surveillance Capitalism Moves Faster Than Tech Regulation

Surveillance technology now collects human behavioral data at an unprecedented scale, a phenomenon which Dr. Shoshana Zuboff attributes to the rise of surveillance capitalism.[30] She defines surveillance capitalism as "the unilateral claiming of private human experience as free raw material for translation into behavioral data" and offers as one unsettling example: "breathing machines purchased by people with sleep apnea . . . secretly sending usage data to health insurers, where the information can be used to justify reduced insurance payments."[31] As its name suggests, surveillance capitalism is driven by private corporations, although products like Ring explicitly offer that data to law enforcement agencies.

What began as data collection necessary to personalize online advertising has since mutated into data collection to create habit-forming products and services, driven by a tech industry that Dr. Zuboff asserts has already begun the transition from gathering behavioral data to using that data to direct behavior.[32]

The proliferation of free services like Facebook, Google/YouTube, and Amazon's Neighbors, subscription services like Amazon Prime, Netflix, and Spotify, and smart home devices like Nest, Ring, and Alexa enable the

30. Shoshana Zuboff, *You Are Now Remotely Controlled*, N.Y. TIMES (Jan. 24, 2020), https://www.nytimes.com/2020/01/24/opinion/sunday/surveillance-capitalism.html [https://perma.cc/2DQH-SA9Z]; *e.g.*, Stuart Thompson & Charlie Warzel, *8 Things to Know About Our Investigation Into the Location Business*, N.Y. TIMES (Dec. 19, 2019), (discussing that even children are not safe from surveillance) https://www.nytimes.com/interactive/2019/12/19/opinion/nyt-cellphone-tracking-investigation.html [https://perma.cc/YFE9-6EQX]; IRL *The Surveillance Economy* (Feb. 4, 2019), (identifying the seemingly persistent issue of companies collecting more information than what is needed to improve their products, often allowing for institutionalized injustices) https://irlpodcast.org/season4/episode5/ [https://perma.cc/3HH9-KJWY].

31. John Laidler, *High Tech Is Watching You*, THE HARV. GAZETTE (Mar. 4, 2019), https://news.harvard.edu/gazette/story/2019/03/harvard-professor-says-surveillance-capitalism-is-undermining-democracy/ [https://perma.cc/25CE-WHJH].

32. *See* John Naughton, *'The Goal Is to Automate Us': Welcome to the Age of Surveillance Capitalism*, GUARDIAN (Jan. 20, 2019), https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook [https://perma.cc/KE9Z-J5DE].

collection of loads of behavioral data about individuals and families. And in the case of smart home devices and platforms like Neighbors and Next Door, companies collect data about guests and travelers. As Cambridge Analytica exposed the information of Facebook friends who never consented[33] to take the now-infamous personality quiz,[34] so too will these devices and platforms likely develop profiles on subjects who are unwitting and unwilling at the time of collection. And where tools permit sharing surveillance data with law enforcement, this can exacerbate our country's existing problems with racially-motivated requests for police presence.[35]

As the initial sleep apnea example illustrated, surveillance capitalism is not at all limited to use by law enforcement,[36] but for privacy advocates, this use by law enforcement is among the more troubling applications of these technologies. This is because (1) the technology is not always reliable (often in inequitable ways that can harm people experiencing homelessness, people of color, and undocumented immigrants);[37] (2) even where it is reliable the process required to achieve such reliability may not be followed;[38] and (3) even where the required process is followed to ensure reliability, the

33. *See AG Racine Sues Facebook for Failing to Protect Millions of Users' Data*, OFF. ATT'Y GEN. D.C. (Dec. 19, 2018), https://oag.dc.gov/release/ag-racine-sues-facebook-failing-protect-millions [https://perma.cc/VHW9-EG58] [hereinafter *AG Racine Sues Facebook*].

34. *See* Carole Cadwalladr & Emma Graham-Harrison, *How Cambridge Analytics Turned Facebook 'Likes' Into a Lucrative Political Tool*, THE GUARDIAN (Mar. 17, 2018), https://www.theguardian.com/technology/2018/mar/17/facebook-cambridge-analytica-kogan-data-algorithm [https://perma.cc/6CAN-HBVZ].

35. *See* Daniel Victor, *When White People Call the Police on Black People*, N.Y. TIMES (May 11, 2018), https://www.nytimes.com/2018/05/11/us/black-white-police.html [https://perma.cc/DA84-3GXT].

36. *See* Kashmir Hill, *I Got Access to My Secret Consumer Score. Now You Can Get Yours, Too*, N.Y. TIMES (Nov. 4, 2019), https://www.nytimes.com/2019/11/04/business/secret-consumer-score-access.html [https://perma.cc/NF87-6Z4G].

37. *See, e.g.*, Caroline Haskins, *Amazon's Home Security Company Is Turning Everyone Into Cops*, VICE (Feb. 7, 2019), https://www.vice.com/en_us/article/qvyvzd/amazons-home-security-company-is-turning-everyone-into-cops [https://perma.cc/P8L2-YXD2]; Rick Paulus, *On Nextdoor, the Homeless Are the Enemy*, ONEZERO (Sept. 30 2019), https://onezero.medium.com/how-nextdoor-encourages-hate-of-the-homeless-9200475cda43 [https://perma.cc/A4VV-XZYU]; Hiba Ali, *Amazon's Surveillance System Is a Global Risk to People of Color*, ZORA (Sept. 25, 2019), https://zora.medium.com/amazons-surveillance-system-is-a-global-risk-to-people-of-color-a5030a19d5e1 [https://perma.cc/536J-HB55].

38. *E.g.*, Clare Garvie, *Garbage In, Garbage Out*, GEO. L. CTR. PRIV. & TECH. (May 16, 2019), (discussing that in one instance, police implemented FR tech on a picture of Woody Harrelson because an officer believed the suspect looked like the celebrity, yet using FR tech on the actual picture of the suspect yielded no results) https://www.flawedfacedata.com/ [https://perma.cc/LDM4-Y6CT].

technology can still be used for purposes and by agencies other than those for which it was initially intended.[39]

Vendor relationships where law enforcement use of surveillance technology is concerned are notoriously lacking in transparency and accountability.[40] In the absence of regulation, this has led to the growth of local Community Control Over Police Surveillance (CCOPS) organizations,[41] which call for greater transparency regarding law enforcement's use of surveillance technology.[42]

---

39. These practices include the police departments with whom consumers share Ring data passing that data along to other agencies, as well as Amazon sharing the information with employees in other countries for human annotation of captured video feeds to train its recognition capabilities. *See, e.g.*, Alfred Ng, *You Shared Ring Footage With Police. They May Share It, Too*, CNET (Sept. 4, 2019), https://www.cnet.com/news/you-shared-ring-footage-with-police-they-may-share-it-too/ [https://perma.cc/K3HN-3KFK]. (discussing police departments not disclosing to consumers when sharing their videos on to other agencies); Brad Heath, *Police Secretly Track Cellphones to Solve Routine Crimes*, USA TODAY (Aug. 23, 2015), https://www.usatoday.com/story/news/2015/08/23/baltimore-police-stingray-cell-surveillance/31994181/ [https://perma.cc/8VB6-EAC5] (discussing police departments using national security technology to solve petty crimes); Nicole Nguyen & Ryan Mac, *Ring Says It Doesn't Use Facial Recognition, But It Has "A Head of Face Recognition Research"*, BUZZFEED NEWS (Aug. 30, 2019), https://www.buzzfeednews.com/article/nicolenguyen/amazon-ring-facial-recognition-ukraine [https://perma.cc/BK3F-6XBL] (discussing that Amazon uses Ring footage to train facial recognition AI); Dell Cameron, *Cops Are Giving Amazon's Ring Your Real-Time 911 Caller Data*, GIZMODO (Aug. 1, 2019). https://gizmodo.com/cops-are-giving-amazons-ring-your-real-time-911-data-1836883867 (discussing police sharing 911 call data, including location data, with Ring).

40. *See, e.g.*, Monte Reel, *Secret Cameras Record Baltimore's Every Move From Above*, BLOOMBERG BUSINESSWEEK (Aug. 23, 2016), https://www.bloomberg.com/features/2016-baltimore-secret-surveillance/ [https://perma.cc/7XJV-ATJK]; *see also Emily* Sullivan, *Baltimore Spending Board Terminates Controversial Surveillance Plane Contract* (Feb. 3, 2021), https://www.wypr.org/post/baltimore-spending-board-terminates-controversial-surveillance-plane-contract (discussing that the program has been discontinued).

41. *Community Control Over Police Surveillance*, ACLU, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/community-control-over-police-surveillance (last accessed Jan. 26, 2020) [https://perma.cc/PGW4-M8YU]; *e.g.*, *Community Oversight of Surveillance – DC*, ACLU D.C., https://www.acludc.org/en/community-oversight-surveillance-dc (discussing such a program proposed in D.C., the Community Oversight of Surveillance (DC COS)) (last visited Jan. 26, 2020) [https://perma.cc/Z6HT-VXBB]; SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT, https://www.stopspying.org/ (discussing such a program in New York City, the Surveillance Technology Oversight Project (STOP)) (last accessed Jan. 26, 2020) [https://perma.cc/TZ5X-KF7J].

42. *See generally* Kade Crockford, *Emails Show Surveillance Oversight Laws Can Stop Secret Police-Amazon Agreements in Their Tracks*, ACLU MASS. (Sept. 10, 2019), https://www.aclum.org/en/publications/emails-show-surveillance-oversight-laws-can-stop-secret-police-amazon-agreements-their (showing that one such group in Massachusetts is encouraged by early results from its civilian oversight efforts).

B. Changing the Calculus on Incentivized Consent for Surveillance

Amazon is particularly problematic because it operates at a national level, but there are still relevant privacy concerns when the data collection is limited to the local level, for instance in the District of Columbia.

Predating Amazon's relationships with police departments, D.C. has used aggressive rebate and voucher programs to encourage citizens to deploy private security cameras.[43] Participation in this program lets the police know which residences installed these devices and capitalizes on a feeling of reciprocity when the police request data from the owner, as the city helped to subsidize the owner's acquisition of the camera. On the one hand, this exacerbates existing suspicions in the community, as law-abiding outsiders to the community (or even tenants, children, and protestors, in their own community[44]) do not get a say over how their image is captured and shared with law enforcement. On the other hand, these kinds of programs increase access to technology that can alleviate fears about lack of security among homeowners, and in D.C.'s case, tenants as well. These kinds of policies incentivize protecting known property interests at the expense of protecting the civil liberties of unknown people.

But surely when entire communities are on the same platform, one which owns all of that surveillance data, as in the case of tech giants like Amazon, that calculus must change.

C. State Consumer Protection Agencies Must Continue to Lead

Although there is interest in regulating this technology at the federal level, no meaningful, relevant legislation has yet been passed. That said, state attorneys general have shown no lack of boldness in bringing antitrust suits against global tech giants like Facebook and Google for their collection and

43. *See Private Security Camera System Incentive Program*, OFF. OF VICTIM SERVS. AND JUST. GRANTS, https://ovsjg.dc.gov/service/private-security-camera-system-incentive-program (last accessed Jan. 26, 2020) [https://perma.cc/8GTL-6N56].

44. Although not specific to DC, the Neighbors app has been known to host posts featuring videos of children walking down the street with a narrator saying, "Whose kids are these?", *see* Drew Harwell, *Ring and Nest Helped Normalize American Surveillance and Turned Us Into a Nation of Voyeurs*, WASH. POST (Feb. 18, 2020), https://www.washingtonpost.com/technology/2020/02/18/ring-nest-surveillance-doorbell-camera/ [https://perma.cc/7965-7Q9W]. Additionally, in 2020, the LAPD requested Ring footage in conjunction with Black-led protests in response to police violence. *See* Matthew Guariglia & Dave Maass, *LAPD Requested Footage of Black Lives Matter Protests*, ELEC. FRONTIER FOUND. (Feb. 16, 2021), https://www.eff.org/deeplinks/2021/02/lapd-requested-ring-footage-black-lives-matter-protests. Fewer than 7% of these protests resulted in violence, destruction, or serious uses of force by police. Kevin Rector, *LAPD Reports Show That the Vast Majority of George Floyd Protests Were Peaceful*, LOS ANGELES TIMES (Oct. 23, 2020), https://www.latimes.com/california/story/2020-10-23/lapd-most-george-floyd-protests-peaceful.

alleged misuse of consumer data.[45] The self-imposed moratoria by Amazon, Microsoft, and IBM shortly before the public announcement of the first false arrests in Michigan[46] in 2020 demonstrate both the prematurity of the widespread deployment of this technology and the privacy gains from heightened public awareness of how these technologies are actually used. To the extent that there are statutory facial recognition bans and oversight initiatives, they are primarily at the local level. While a federal solution would be preferable from a civil rights and social justice perspective, the fastest way to bring the law up to speed with technology and with business practices is by focusing on efforts at the state and local level.

IV. THE LAW'S RESPONSE

A. Traditional Legal Remedies Do Not Apply

Contract, constitutional, and property law are unlikely to remedy the privacy issues associated with Amazon's technology.

The Fourth Amendment does not apply when the search is conducted by a private party (e.g., the homeowner). One ACLU attorney, Matt Cagle, has observed:

45. *See, e.g.*, Shannon Bond & Bobby Allyn, *48 AGs, FTC Sue Facebook, Alleging Illegal Power Grabs to 'Neutralize' Rivals*, NPR (Dec. 9, 2020), https://www.npr.org/2020/12/09/944073889/48-attorneys-general-sue-facebook-alleging-illegal-power-grabs-to-neutralize-riv [https://perma.cc/L77A-Y8CA]; Catherine Thorbecke & Aaron Katersky, *Google Hit With New Antitrust Lawsuit From 38 State Attorneys General*, ABC NEWS (Dec. 17, 2020), https://abcnews.go.com/Technology/google-hit-antitrust-lawsuit-38-state-attorneys-general/story?id=74780182 [https://perma.cc/QKR8-FMBX].

46. *See* Rebecca Heilweil, *Big Tech Companies Back Away From Selling Facial Recognition to Police. That's Progress*, VOX (June 11, 2020), https://www.vox.com/recode/2020/6/10/21287194/amazon-microsoft-ibm-facial-recognition-moratorium-police; Robert Williams, *I Was Wrongfully Arrested Because of Facial Recognition. Why Are Police Allowed to Use It?*, WASH. POST (June 24, 2020), https://www.washingtonpost.com/opinions/2020/06/24/i-was-wrongfully-arrested-because-facial-recognition-why-are-police-allowed-use-this-technology/ [https://perma.cc/W2LW-SJTQ]. Less than thirty days after Robert William's op-ed, Engadget published a story describing a second false arrest prompted by police use of facial recognition technology. See Holt, *supra* note 16.

> [T]he simple existence of a program like the Neighbors Portal threatens to blur, if not eliminate, the distinction between private-sector surveillance services and the government's role as enforcer of the law. With regards to the latter, we have powerful constitutional safeguards, while with the former we have only terms of service and privacy policy agreements that no one reads.[47]

To that end, per its terms of service, Ring's rights to the footage taken from a user's front door include "an unlimited, irrevocable, fully paid, and royalty-free, perpetual, worldwide right to re-use, distribute [sic] store, delete, translate, copy, modify, display, sell, create derivative works."[48]

Although Ring has indicated that it would not provide user video data in response to a subpoena,[49] if a user willingly gives up their own data, that would also be a means of side-stepping constitutional safeguards.[50] One scholar has additionally observed, in a manner consistent with the ACLU's concerns, that use of corporate surveillance products in criminal investigations could shield proffered evidence from cross-examination by the defendant due to trade secret and/or intellectual property protections.[51]

Property law offers no redress either, as Ring disclaims any responsibility for the user's improper deployment of the product. "Our devices are not intended to be and should not be installed where the camera is recording someone else's property without prior consent nor public areas."[52] In the context of Amazon's facial recognition product, Rekognition, even an Amazon employee has taken issue with this approach. "For Amazon to say that we require our Rekognition customers to follow the law is no guarantee of civil liberties at all—it's a way to avoid taking responsibility for

---

47. Sam Biddle, *Amazon's Home Surveillance Chief Declared War on 'Dirtbag Criminals' As Company Got Closer to Police*, INTERCEPT_ (Feb. 14, 2019), https://theintercept.com/2019/02/14/amazon-ring-police-surveillance/ [https://perma.cc/BT2X-2SUL].

48. Guariglia, *supra* note 28.

49. Drew Harwell, *Doorbell-Camera Firm Ring Has Partnered With 400 Police Forces, Extending Surveillance Concerns*, WASH. POST (Aug. 28, 2019), https://www.washingtonpost.com/technology/2019/08/28/doorbell-camera-firm-ring-has-partnered-with-police-forces-extending-surveillance-reach/ [https://perma.cc/NWS2-FAQV]; *How Law Enforcement Uses the Neighbors App*, RING HELP, https://support.ring.com/hc/en-us/articles/360031595491 (last visited Jan. 26, 2020) [https://perma.cc/E9XH-FBEQ].

50. *See Fight for the Future Launches New Campaign Calling on Mayors and City Officials To Ban Police Partnerships With Amazon Ring Surveillance Doorbells*, FIGHT FOR THE FUTURE (July 31, 2019), https://www.fightforthefuture.org/news/2019-07-31-fight-for-the-future-launches-new-campaign-calling/ [https://perma.cc/C5RH-WZXT] [hereinafter Fight for the Future].

51. Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 STANFORD L. REV. 1343 (May 2018), https://review.law.stanford.edu/wp-content/uploads/sites/3/2018/06/70-Stan.-L.-Rev.-1343.pdf [https://perma.cc/MEV7-JEG7]*; cf.* Charlie Warzel, *Privacy Is Too Big to Understand*, N.Y. TIMES (Apr. 16, 2019), https://www.nytimes.com/2019/04/16/opinion/privacy-technology.html [https://perma.cc/DH6L-36FT].

52. Biddle, *supra* note 47.

the negative uses of this technology."[53] This presents two problems. First, coupled with the contract law issues discussed above, this means that Amazon is not responsible for information collected by Ring but has the freedom to use that information as it sees fit. Second, one-click consent[54] allows for an end run to be made around the Fourth Amendment's protections, as homeowners can share their surveillance data with law enforcement. Indeed, in response to public concern about police in Jackson, Mississippi piloting a program that harvests Ring data from homeowners in real-time, Amazon offered the following:

> [Amazon and Ring] are not involved in any way with any of the companies or the city in connection with the pilot program. The companies, the police and the city that were discussed in the article do not have access to Ring's systems or the Neighbors App. Ring customers have control and ownership of their devices and videos, and can choose to allow access as they wish.[55]

B. There is a Pressing Need for Alternative Remedies

One might argue that the response of privacy advocates is akin to Chicken Little.[56] Clearly if society feels a grievous harm is happening here, cultural norms and market forces will correct the error. Indeed, this seems to have happened in Orlando, where deployment of Amazon surveillance technology was attempted and discontinued twice.[57] But this is not an issue of what technology local police choose to use. It is an issue of what technologies police encourage consumer-citizens to use, particularly after police departments sign agreements that prohibit them from making any public statement about the technology without company approval.

> If media reaches out with questions about the partnership or the Neighbors app, or for assistance with overall PR strategy, please contact Ring's PR Coordinator . . . All public facing messaging and materials must be approved by both parties; either by using approved templates or submitting to Ring PR for approval.[58]

53. An Amazon Employee, *supra* note 19.

54. Harwell, *supra* note 3.

55. Guariglia, *supra* note 23.

56. "Chicken Little" is a folk tale about a chicken who believes the sky is falling and becomes hysterical with concern that the world is coming to an end after an acorn drops on their head.

57. Nick Statt, *Orlando Police Once Again Ditch Facial Recognition Software*, VERGE (July 18, 2019), https://www.theverge.com/2019/7/18/20700072/amazon-rekognition-pilot-program-orlando-florida-law-enforcement-ended [https://perma.cc/Q934-AYTQ].

58. Letter from Corey Williamsen, Freedom of Info. Officer, Vill. of Benseville, to Shreyas Gandlur 8 (Aug. 13, 2019), https://www.documentcloud.org/documents/6359444-Bensenville-IL-Emails.html. [https://perma.cc/9NN2-8PGX].

The average citizen will interpret a remark made by the police, who are sworn to serve and protect the public, as a remark made in the interest of public safety, not as public relations for Amazon coming to the consumer-citizen through the mouthpiece of their local police department. Not only is this unethical, but if people knew the truth about this practice, it could diminish public trust in local police departments. Regardless, a situation in which the police can only make positive statements about a consumer product interferes with the free market for that product.[59]

However, at present, the momentum of surveillance capitalism is nudging corporations towards more expansive clandestine data collection and usage, and the homeowners purchasing Amazon Ring units have a stronger incentive to protect their online orders than the legal rights of strangers. As such, waiting for cultural norms and market correction without additional intervention will allow for continuing privacy harms.

C. The Case for Consumer Protection

The underlying issues surrounding Ring are further exacerbated by the fact that Amazon financially incentivizes police departments to encourage citizens to sign up for the Neighbors app. Amazon does this by offering departments credits towards purchasing Ring units—which police can then sell to citizens at a rate much lower than citizens would get from Amazon directly—proportionate to the number of Neighbors app downloads by citizens in their jurisdiction.[60] However, this exacerbation is one basis upon which consumer protection law may provide a remedy.

State Unfair and Deceptive Acts and Practices (UDAP) laws and the FTC's Endorsement Guides can provide some recourse where contract, property, and constitutional law offer no relief.[61] One of the chief concerns of consumer protection law is misleading statements in product promotions, including insufficient substantiation for efficacy claims and the omission of facts that might inform a purchasing decision (and in some jurisdictions, the

59. Additionally, as an international industry association for surveillance equipment noted, Amazon's behavior lacks transparency in ways that harm the industry as a whole. "We are troubled by recent reports of agreements 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." 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/ [https://perma.cc/H4MK-2UXQ].

60. Caroline Haskins, *Amazon Requires Police to Shill Surveillance Cameras in Secret Agreement*, VICE: MOTHERBOARD, (July 25, 2019, 11:54 AM), https://www.vice.com/en_us/article/mb88za/amazon-requires-police-to-shill-surveillance-cameras-in-secret-agreement [https://perma.cc/8M8Z-AK84].

61. The Lanham Act, codified in part in 15 U.S.C. § 1125(a)(1), could also apply here, as it allows companies to bring suit against their competitors for deceptive practices, on the premise that consumers are purchasing from the deceptive seller rather than the honest seller, costing the honest seller market share and profits as a result of their adhering to honest practices. 15 U.S.C. § 1125 (2018). The Lanham Act is not a primary focus of this Note, as it is a consumer protection vehicle usable only by a competitor surveillance technology company.

reason for a merchant to offer a discount).[62] The FTC's Endorsement Guides indicate, among other things, that when promoting a company's product, the promoter must disclose any benefit they have received from the company in exchange for that promotion, and that the company (Amazon in this instance) can be liable if the promoter or endorser fails to do so.[63] This issue is complicated when partnerships with police departments are concerned, as consumer protection agencies are sometimes barred from bringing legal actions against police departments. Where the corporate entity has editorial authority over what the police department says on social media and in other public statements about the company's surveillance products, that company should be liable for that endorser's statements about those products.

1. UDAP Statutes – Active Law Across All States and D.C.

As noted above, state and local governments enacted UDAP statutes to help protect consumers from deceptive trade practices by merchants. The D.C. UDAP statute, for instance, is called the Consumer Protection Procedures Act (CPPA). CPPA protects D.C. consumers—persons who create the economic demand for a trade practice (other than for the purpose of resale)—from unfair or deceptive trade practices.[64] CPPA protects consumers by providing a private right of action against merchants—persons who sell, lease, or transfer consumer goods or services, directly or indirectly, in the ordinary course of business, or who supply goods and services which would be the subject matter of a trade practice.[65] As an example, D.C.'s Office of the Attorney General brought suit on behalf of D.C. residents against Facebook for the now-infamous Cambridge Analytica incident by filing a complaint for violations of CPPA.[66]

While it seems clear that Amazon could be the subject of a consumer protection suit, interestingly it is also legally possible (though politically unlikely) that a local police department could be sued under CPPA. Under D.C. caselaw, the Metropolitan Police Department (MPD) could be a merchant under CPPA, provided that MPD supplied directly or indirectly consumer goods or services, received remuneration from companies providing consumer goods or services, and/or entered a consumer-merchant relationship.[67] Where jurisdictions have similar UDAP statutes to D.C.'s

62. *See FTC Policy Statement Regarding Advertising Substantiation* (Nov. 23, 1984), https://www.ftc.gov/public-statements/1984/11/ftc-policy-statement-regarding-advertising-substantiation [https://perma.cc/3MYE-FW9Y].

63. Guides Concerning the Use of Endorsements and Testimonials in Advertising, 16 C.F.R. § 255.5 (2020).

64. The D.C. Code gives weight to the FTC's interpretations of 15 U.S.C. § 45(a) here. D.C. CODE ANN. § 28-3901(b) (West).

65. D.C. CODE ANN. § 28-3901 (West) [hereinafter CPPA].

66. *AG Racine Sues Facebook*, *supra* note 33.

67. *See* Snowder v. D.C., 949 A.2d 590, 599–600 (D.C. 2008) (finding DC Metropolitan Police Department not a merchant because it did not supply consumer goods or services, receive remuneration, or enter a consumer-merchant relationship); CPPA § 28–3901(a)(3).

CPPA,[68] police departments in the regular practice of selling Ring units, or even promoting the Neighbors App, could be found to be acting as merchants.

If a violation is found under the CPPA, consumers can sue directly and nonprofit organizations can sue indirectly.[69] Violations in this instance might include "[failure] to state a material fact if such failure tends to mislead"[70] and/or "falsely stat[ing] the reasons for offering or supplying goods or services at sale or discount prices" [71] as police departments are likely disclosing neither the full details of Amazon's editorial authority nor the incentive they receive to promote downloads of the Neighbors App.

The three major challenges with this approach are potential immunity for law enforcement agencies, political infeasibility even where there is not legal immunity, and the heightened burden of proof under UDAP. Consumer protection cases are not civil rights cases, and as such, where law enforcement enjoys immunity from suit, it might create a barrier in holding Amazon liable under a UDAP consumer protection theory. In terms of political feasibility, an AG may not even want to sue Amazon over the behavior of their own police force. Many UDAP statutes require clear and convincing evidence in their burden of proof.[72]

Remedies for UDAP violations vary by jurisdiction. In D.C., the CPPA allows for treble damages (or $1,500 per violation, if greater), as well as punitive damages and attorney's fees. It also allows for an injunction against the unlawful trade practice.[73]

2. FTC Endorsement Guidelines—Federal Guidance Each State Would Need to Adopt as Regulation

Per the FTC's guidance on endorsements, "The same [disclosure] is usually true if the endorser has been paid or given something of value to tout the product. The reason is obvious: Knowing about the connection is important information for anyone evaluating the endorsement."[74] Especially when the endorser is expected to provide unbiased advice about public safety, it is particularly important that any connection related to value (such as

68. As many as 43 seem to come close. *See* Carolyn L. Carter, *Consumer Protection in the States*, NAT'L CONSUMER L. CTR. 12 (Feb. 2009), https://www.nclc.org/images/pdf/udap/report_50_states.pdf [https://perma.cc/8KMZ-XTWG].

69. D.C. CODE § 28–3901.

70. D.C. CODE § 28–3904(f).

71. D.C. CODE § 28–3904(l).

72. *See* Carter, *supra* note 68, at 24–29.

73. *District of Columbia Consumer Protection Laws*, OFF. OF THE ATT'Y GEN. OF D.C., https://oag.dc.gov/consumer-protection/other-consumer-help-agencies-and-websites/submit-consumer-complaint/district-columbia-consumer-protection-laws (last accessed Jan. 26, 2020) [https://perma.cc/8AJR-QGQB].

74. Additionally, nothing in the FTC's Endorsement Guides states that these endorsements are limited to commentary on social media. *The FTC's Endorsement Guides: What People Are Asking*, FED. TRADE COMM'N (2017), https://www.ftc.gov/tips-advice/business-center/guidance/ftcs-endorsement-guides-what-people-are-asking [https://perma.cc/7JP9-J4DR].

discounts on products proportionate to app downloads) be disclosed clearly and conspicuously.

Due to the level of control Amazon has over public statements by police departments, it is unlikely that Ring would be able to evade responsibility under this theory:

> It's unrealistic to expect [a company] to be aware of every single statement made by a member of [its] network. But it's up to [the company] to make a reasonable effort to know what participants in [the company's] network are saying. That said, it's unlikely that the activity of a rogue blogger would be the basis of a law enforcement action if your company has a reasonable training, monitoring, and compliance program in place.[75]

However, the FTC itself cannot pursue action against local police departments. State and local governments could adopt standards akin to the FTC's endorsement guidelines in enforcing their UDAP statutes. This would enable them to pursue Amazon for consumer protection violations that the tech company permitted (encouraged, arguably) through the sales tactics utilized by its endorsers, local police departments.[76]

In terms of remedies at the FTC level, if the company entered into a consent order to stop the deceptive act or practice, it could be fined more than $10,000 for each subsequent violation.[77]

3. Practical Limitations of the Consumer Protection Approaches

These consumer protection remedies are likely to be unsatisfying to privacy advocates, who are rightly concerned about systemic abuses in the criminal justice system.[78] Additionally, these remedies do not provide a real opportunity for the non-consumer passerby passively captured on video to

75. *Id.*

76. New York's Attorney General, for instance, has enforcedagainst misconduct similar to the misconduct covered by the FTC's Endorsement Guides, albeit under a different theory. *See New York Attorney General Cracks Down on Falsified Online Reviews*, INFOLAWGROUP, https://www.infolawgroup.com/insights/2013/10/articles/ftc/ny-ag-cracks-down-on-fake-reviews (last accessed Apr. 14, 2020) [https://perma.cc/HG6V-WPLR].

77. 15 U.S.C. § 45.

78. Telephone Interview with Andrew Ferguson, Professor, David A. Clarke Sch. of L. (Nov. 14, 2019).

bring suit.[79] Some UDAP statutes permit nonprofits to bring suits on behalf of consumers. Some may only permit consumers themselves to sue. However, in the absence of federal privacy legislation that accounts for second order biometric privacy threats, that is the best existing law can offer.[80]

D. Other Public Policy Considerations

Although outside the scope of the consumer protection law solutions proposed by this Note, there are other social and cultural issues which may serve as effective messaging points for rallying public support in defense of community oversight of these kinds of surveillance partnerships. One group has created a product warning site listing some of the concerns consumers may have.[81] VICE has noted the concern taxpayers may have with police departments subsidizing the purchase of Ring units,[82] as has the Electronic Frontier Foundation. For example, the EFF has explained that municipalities are "paying Amazon up to $100,000 to reduce costs of Ring cameras by $50 or $100 for city residents."[83]

Some might find it unsavory that Amazon uses doorbell camera data to capitalize on viral video behavior to drive sales.[84] The New York Times compellingly reports on the relationship between Ring and Neighbors, listing numerous examples of scary, funny, and sweet videos captured by Ring and

79. It is only a matter of time until technology like Ring makes situations like deploying police against delivery drivers more efficient. *See* Mariel Padilla, *Black Deliveryman Says He Was Blocked and Interrogated by White Driver*, N.Y. TIMES (May 17, 2020), https://www.nytimes.com/2020/05/17/us/black-delivery-driver-okc-travis-miller.html [https://perma.cc/97ST-7Y3H]. It seems unlikely that Amazon would call for swift investigation when a competitor's delivery service falls victim to Ring-based police deployment. *See* Sven Gustafon, *Police in Detroit Suburb Pin Black Amazon Driver in Incident Over Parking*, MSN: AUTOBLOG (June 10, 2020), https://www.msn.com/en-us/autos/news/police-in-detroit-suburb-pin-black-amazon-driver-in-incident-over-parking/ar-BB15jsTT [https://perma.cc/NL8Q-6QE3].

80. Another example of second order privacy threats can be seen in commercial genetic databases. *See* Megan Molteni, *The Future of Crime-Fighting Is Family Tree Forensics*, WIRED (Dec. 26, 2018), ("[D]atabases like GEDMatch [are expected] to grow so big in the next few years that it will be possible to find anyone from just their DNA, even if they haven't voluntarily put it in the public domain") https://www.wired.com/story/the-future-of-crime-fighting-is-family-tree-forensics/ [https://perma.cc/4RDB-K3C3].

81. *Amazon Ring Cameras Are Not Safe*, https://www.ringsafetywarning.com/ (last accessed Jan. 26, 2020) [https://perma.cc/TUW8-9GNE].

82. Caroline Haskins, *US Cities Are Helping People Buy Amazon Surveillance Cameras Using Taxpayer Money*, VICE (Aug. 2, 2019), https://www.vice.com/en_us/article/d3ag37/us-cities-are-helping-people-buy-amazon-surveillance-cameras-using-taxpayer-money [https://perma.cc/59SS-EDK9].

83. Matthew Guariglia, *Five Concerns about Amazon Ring's Deals with Police*, EFF (Aug. 30, 2019), https://www.eff.org/deeplinks/2019/08/five-concerns-about-amazon-rings-deals-police [https://perma.cc/UC69-VNUF].

84. *See* Ben Fox Rubin, *How Ring's Neighbors App Is Making Home Security a Social Thing*, CNET (Dec. 3, 2018), https://www.cnet.com/news/how-rings-neighbors-app-is-making-home-security-a-social-thing/ [https://perma.cc/6G48-PKFF].

shared on Neighbors.[85] Looking towards the future of what the normalization of this kind of technology could lead to, Evan Greer of Fight for the Future, a privacy advocacy group, has argued:

> Amazon is building a privately run, for-profit surveillance state, and they're getting local police to market it for them in exchange for VIP access to the panopticon . . . This corporate and government overstep allows law enforcement agencies to side-step judicial oversight by asking customers to give up their privacy rights by sharing confidential information with local police departments.[86]

Other commentators have voiced concerns with how Ring's proposed "suspicious activity detection" will be deployed[87] with enhanced biometrics (beyond facial recognition)[88] and with constant omnipresent surveillance due to density of devices.

> O'Sullivan suggests that the ubiquity of devices means you could be surveilled by Amazon even if you don't own its products. "If you have enough Ring doorbell cameras on your block, it doesn't matter if you bought one or not; you're being monitored and, down the road, perhaps your device is pinging them.[89]

When government agencies make a mistake due to dysfunctional technology, courts can opt not to suppress evidence obtained from it under the "good faith" exception. [90] There are several instances of innocent individuals who, through unfortunate coincidence, were captured by the surveillance apparatus and were subject to undue police scrutiny. As Bruce

---

85. *See* John Herrman, *Who's Watching Your Porch?*, N.Y. TIMES (Jan. 19, 2020), https://www.nytimes.com/2020/01/19/style/ring-video-doorbell-home-security.html [https://perma.cc/77GA-ASK4].

86. Fight for the Future, *supra* note 50. Some would remedy the lack of judicial oversight by requiring civilian oversight, *see Community Control Over Police Surveillance supra* note 41.

87. Biddle, *supra* note 47, "Amazon's Home Surveillance Chief…"

88. *See* Madhumita Murgia, *Who's Using Your Face? The Ugly Truth About Facial Recognition*, FIN. TIMES (Sept. 18, 2019), https://www.ft.com/content/cf19b956-60a2-11e9-b285-3acd5d43599e [https://perma.cc/5Q57-WDFL].

89. Charlie Warzel, *Amazon Wants to Surveil Your Dog*, N.Y. TIMES (Oct. 1, 2019), https://www.nytimes.com/2019/10/01/opinion/amazon-privacy.html. [https://perma.cc/VK7A-4GKG]. Relatedly, Brad Smith, President of Microsoft, has observed that "[w]hen combined with ubiquitous cameras and massive computing power and storage in the cloud, a government could use facial recognition technology to enable continuous surveillance of specific individuals. It could follow anyone anywhere, or for that matter, everyone everywhere." Amitai Etzioni, *Facial Recognition Meets the Fourth Amendment Test*, YAHOO! NEWS (Sept. 22, 2019) https://news.yahoo.com/facial-recognition-meets-fourth-amendment-191500422.html [https://perma.cc/28FZ-BWHU].

90. *See* Herring v. United States, 555 U.S. 135, 146–47 (2009) (noting recklessly maintained database might justify excluding evidence obtained due to inaccurate information, but isolated instances of negligence do not).

Schneier, cybersecurity expert, notes: we need to consider where the tradeoff ends for the security of property.[91]

V. FRICTION IS THE BEST NEAR-TERM SOLUTION

Because traditional claims under contract, property, and constitutional law likely favor Amazon, until robust federal privacy legislation passes, consumer protection law may be the only method for slowing corporate-facilitated police surveillance—namely by using local UDAP statutes and/or adopting and enforcing provisions like the FTC's Endorsement Guides at a local level. These methods can result in courts issuing financial penalties against Amazon as well as injunctions requiring greater transparency from Amazon, specifically regarding the representations made by police departments in the marketplace about the Ring product and the nature of the relationship between their department and Amazon. While privacy advocates would likely prefer to challenge the type of data collected or method of collection altogether, such action would require an immense amount of public education and debate. Only then could Congress pass federal legislation.

As such, to provide as immediate a stopgap as possible until that lengthy process can be completed, the best approach is to create friction in the sales growth of products like Amazon Ring and in the processes used by the police departments deputized as sales teams by tech giants like Amazon.

A. The Limits of Actionable Conduct Under Consumer Protection Law

Although privacy advocates are concerned with law enforcement making an end-run around the Constitution, a consumer protection law approach to the problem posed by corporate-law enforcement partnerships (such as Amazon Ring and local police departments) would not reach that far, only addressing problems such as:

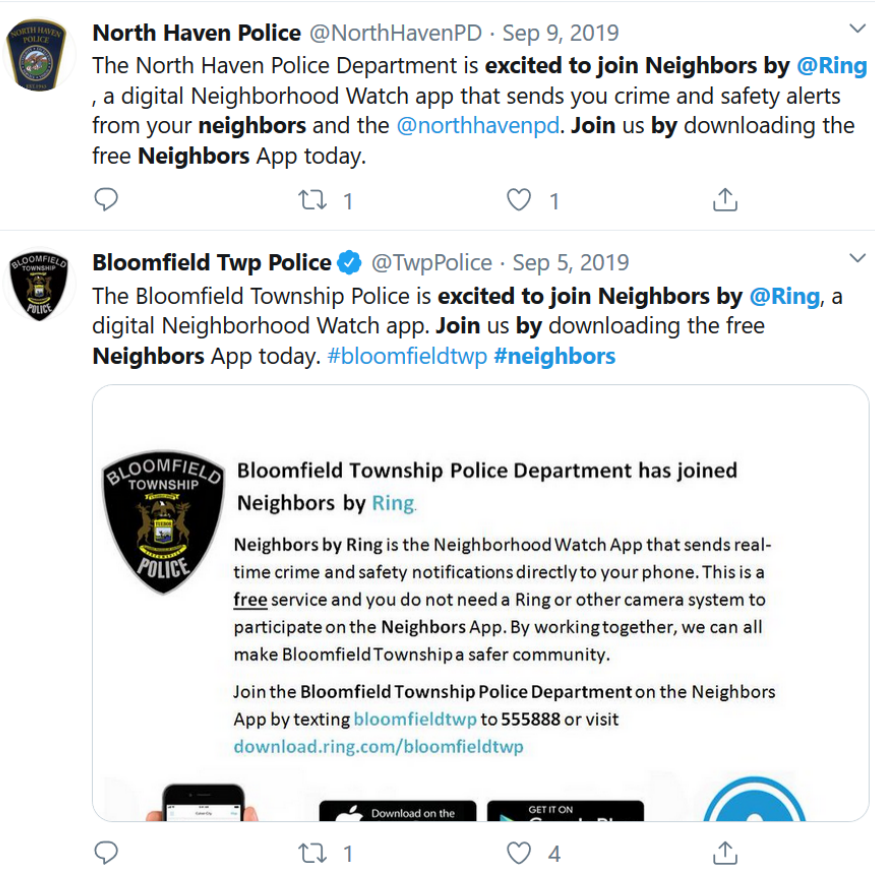
91. *See* Schneier, *supra* note 26; Jennifer Valentino-DeVries, *Tracking Phones, Google Is a Dragnet for the Police*, N.Y. TIMES (Apr. 13, 2019), https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html [https://perma.cc/UWC7-XMBY].

1) Misrepresentations or omissions by police departments about motivations for encouraging residents to download the Neighbors app, and relatedly, of discounted Ring units available directly or indirectly through the police department;
2) Misrepresentations or omissions by police departments about the nature of their agreement to work with Amazon Ring, specifically the editorial authority Amazon has over police departments' public statements regarding the Ring product;
3) Misrepresentations by Amazon Ring about the effectiveness of its product;
4) Misrepresentations or omissions by Amazon Ring about its privacy policies, specifically what data it collects from users and how it uses the data it collects from users;
5) Misrepresentations or omissions by Amazon Ring about the security of its product;
6) Harms to competitors (who likely also sell smart home surveillance products but do so without utilizing misleading partnerships with local police departments).

Amazon has partnered with more than 400 police departments,[92] a partnership which entails promoting Ring products (including the Neighbors app) on official police channels. "All partnerships require police to get all public statements about Ring approved by the company first, as Gizmodo reported. Police are also given a series of scripts by Ring which lay out how police are supposed to talk about the company on Neighbors."[93]

92. Jamie Siminoff, *Working Together for Safer Neighborhoods: Introducing the Neighbors Active Law Enforcement Map*, RING: BLOG (Aug. 28, 2019), https://blog.ring.com/2019/08/28/working-together-for-safer-neighborhoods-introducing-the-neighbors-active-law-enforcement-map/ [https://perma.cc/YUV2-NAVN]. More recent reports suggest this number may be closer to 2,000 as of 2021, *see* Lyons, *supra* note 23.

93. Caroline Haskins, *Ring Says It's Partnered with 405 Police Departments, Here's What We Know*, VICE (Aug. 28, 2019), https://www.vice.com/en_us/article/a35vy4/ring-says-its-partnered-with-405-police-departments-heres-what-we-still-dont-know [https://perma.cc/2SQG-46H6].



These promotions often conspicuously leave out a material motivation for the encouragement to download (i.e., discounted Ring units), which would have been a clear violation of the FTC's endorsement guidelines had the endorsing party been subject to the FTC's authority.[94]

Regarding editorial authority, Wired reported one instance from a New Jersey police department that highlighted the company's level of control over public statements:

94. *See* Antonio Villas-Boas, *Amazon Requires Police Departments To Advertise Ring Home Security Products to Residents In Return for Free Ring Cameras*, BUS. INSIDER (July 25, 2019), https://www.businessinsider.com/amazon-ring-require-police-advertise-for-free-ring-cameras-2019-7 [https://perma.cc/DU9N-4772].

> 'Unfortunately I can't make [the mayor and public safety director] say anything specific,' Bloomfield Police Captain Vincent Kerney wrote back to the Ring staffer. 'All of the information was copied and pasted directly from your press releases with the exception of the quotes.' The Ring public relations representative insisted the changes be made at least on Facebook, which they later were, according to the post's edit history. The Bloomfield Police Department did not return a request for comment.[95]

Ring's claims about the effectiveness of its product are also potential cause for consumer protection action because its own studies are inadequate, the data from those studies remain undisclosed, and independent studies do not corroborate the company's claims.[96] Amazon has the burden of substantiating its efficacy claims, and it does not seem capable of meeting it. One meta-study from MIT has found that despite Ring's claims of reducing crime, "the only study carried out independently of Ring found that neighborhoods without Ring doorbells were actually less likely to suffer break-ins than those with them." MIT went on to share one expert's questioning of the legitimacy of Ring's own studies. "I don't see the decrease in crime [Ring claims]," says Maria Cuellar, a statistician and assistant professor of criminology at the University of Pennsylvania, referring to the public district-level data. She says the sample size is too small, too: "It's not enough to say whether the effect is something you see in the data, or just some random variation." Other times, Ring did not provide the data that supported its claims when contrary evidence seemed to disprove them. Subsequent reporting on these studies further undercuts their validity as substantiation of crime reduction claims.[97]

There are also potential issues with violations of consumer expectations of privacy and security. In one instance, Amazon shared data with a Ukrainian development team.[98] Police can share users' data with other agencies.[99] Amazon can use it to train their own facial recognition programs and can sell the data to others.[100] And—in a practice that may even subject police to legal

---

95. Louise Matsakis, *Cops Are Offering Ring Doorbell Cameras in Exchange for Info*, WIRED (Aug. 2, 2019), https://www.wired.com/story/cops-offering-ring-doorbell-cameras-for-information/ [https://perma.cc/6ZR6-NN8T].

96. *See, e.g.*, Mark Harris, *Video Doorbell Firm Ring Says Its Devices Slash Crime—But The Evidence Looks Flimsy*, MIT TECH. REV. (Oct. 29, 2018), https://www.technologyreview.com/s/612307/video-doorbell-firm-ring-says-its-devices-slash-crimebut-the-evidence-looks-flimsy/ [https://perma.cc/ET3Q-YK2F].

97. *See* 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.

98. Biddle, *supra* note 47.

99. *See* Ng, supra note 20.

100. Octavio Mares, *How Amazon Is Selling Your Facial Recognition Data Using a Doorbell*, INFO. SEC. NEWSPAPER, (Aug. 14, 2019), https://www.securitynewspaper.com/2019/08/14/how-amazon-is-selling-your-facial-recognition-data-using-a-doorbell/ [https://perma.cc/UT3P-VABE].

action as it represents misuse of sensitive data—police share 911 data with Amazon.[101] Ring also has historically encountered problems with the security of its devices in disturbing ways.[102]

B. Friction and Deterrence through UDAP

Existing state and local UDAP statutes could effectively slow the spread of sales methodologies like those used by Amazon to sell Ring.

As of the time of this writing, Amazon had not yet substantiated its claims of reducing crime or making neighborhoods safer. In fact, the only information publicly available, via third parties, refuted Amazon's claims.[103] By limiting Amazon's ability to make unsubstantiated claims about Ring's effectiveness in reducing crime, police departments may be less likely to form partnerships with Ring, and consumers less likely to purchase Ring units. In jurisdictions where companies are liable for the actions of their endorsers, police departments that repeat Amazon's unsubstantiated claims could give rise to additional liability for Amazon under the local UDAP statute. Where jurisdictions have similar UDAP statutes to D.C.'s CPPA, [104] police departments that sell Ring units or even promote the Neighbors App could be treated as merchants.

Although it may be politically unfeasible to sue a police department, D.C. case law suggests that police departments could violate the CPPA if they supplied services and/or received remuneration for the services provided and/or entered into a consumer-merchant relationship.[105] As noted above,[106] consumers and nonprofits can bring suit in D.C. under its consumer protection statute, and that right of action is common among the states.[107] To the extent that other jurisdictions have similar consumer protection laws, and that their corresponding police departments exhibit the reported behaviors—e.g., neglecting to disclose the discounts received through Neighbor app downloads or directly selling Ring units to residents or receiving remuneration from Amazon for their indirect facilitation of Ring sales—there may be immediately actionable behavior against the police departments and/or against Amazon for the police department's actions under such laws.

The biggest challenge with this approach is if the representations about the product are being made by the police department but not directly by Amazon (even if the communications are approved or pre-written by

101. *See* Cameron, *supra* note 39.

102. *See, e.g.*, Joseph Cox & Samantha Cole, *How Hackers Are Breaking into Ring Cameras*, VICE (Dec. 11, 2019), https://www.vice.com/en_us/article/3a88k5/how-hackers-are-breaking-into-ring-cameras [https://perma.cc/P28G-9PR8].

103. *See, e.g.*, Harris, *supra* note 96; Farivar, *supra* note 97.

104. *See* Carter, *supra* note 68. Violations in this instance might include "[failure] to state a material fact if such failure tends to mislead" and/or "falsely state the reasons for offering or supplying goods or services at sale or discount prices" as police departments are likely not disclosing the full details of Amazon's editorial authority nor the incentive they receive to promote downloads of the Neighbors App. D.C. CODE § 28–3904(f).

105. *See* Snowder v. D.C., 949 A.2d 590, 599–600 (D.C. 2008).

106. D.C. CODE § 28-3901(b).

107. *See* Carter, *supra* note 68.

Amazon), jurisdictions in which police departments are immune from suits by consumer protection agencies may block liability for Amazon as well. In such jurisdictions there would unfortunately still be no recourse, as (1) the company which could be liable is not making the representation to the consumer, (2) the merchant/endorser who cannot be liable is making the representation to the consumer, and (3) the jurisdiction does not permit acts by the immune merchant/endorser to create liability for the company. It is unlikely that any jurisdiction would permit this trifecta of policies, especially when the company has such powerful editorial authority with the merchant/endorser in question as Amazon Ring does with local police departments. At a minimum this does not appear to be the case in D.C., where courts may consider police to be merchants.

An additional challenge is burden of proof, as many UDAP statutes require clear and convincing evidence, which makes it harder to succeed once the court reaches consideration of the merits.

C. Friction and Deterrence Using the FTC's Endorsement Guides as a Model

Even if the FTC could bring claims under the FTC Act against Amazon for endorsements made by police departments,[108] it may be politically unfeasible. While state Attorneys General may encounter similar political obstacles, they have demonstrated their readiness to take on tech giants like Facebook and Google over issues of commodification of consumer data and violations of privacy, and as such, might sue the corporate provider of the surveillance technology, such as Amazon.[109]

As noted above, the FTC's guidance on endorsements requires disclosure when an endorser has "been paid or given something of value to tout the product" and that the company must have a "reasonable training, monitoring, and compliance program in place" to ensure endorser conduct complies with the FTC's guidelines.[110] Because of Amazon's substantial level of control over the communications and representations made by police departments about its Ring product, a state or local government enacting a

108. FTC's jurisdiction is limited to "persons, partnerships, or corporations." 15 U.S.C. § 45(a)(2). Its organic statute defines a corporation as an entity "organized to carry on business for its own profit or that of its members." 15 U.S.C. § 44. Municipal police departments do not fall within this purview.

109. *See* Bond & Allyn, *supra* note 45.

110. FED. TRADE COMM'N, *supra* note 74, at 1, 14; *see also* Letter from Mary K. Engle, Assoc. Dir., Div. of Advert. Pract., Fed. Trade Comm'n, to Aaron Hendleman & Lydia Parnes, Counsel for Nordstrom, Inc. (Feb. 22, 2013) (on file with Fed. Trade Comm'n), https://www.ftc.gov/sites/default/files/documents/closing_letters/nordstrom-rack/130222nordstromrackletter.pdf. Violations of these guidelines can result in enforcement penalties under the Commission's Section 5 authority. *See* Mark S. Goodrich & Jason Howell, *Check in on Influencer Marketing*, CONSUMER PROT. REV. (Aug. 31, 2020), https://www.consumerprotectionreview.com/2020/08/check-in-on-influencer-marketing/ [https://perma.cc/ZC9U-EY6P]; Richard B. Newman, *Another Lesson From the Federal Trade Commission on Endorsement Guideline Compliance*, FTC DEF. LAW. (Nov. 16, 2018), https://ftcdefenselawyer.com/another-lesson-from-federal-trade-commission-endorsement-guideline-compliance/ [https://perma.cc/V288-XNNQ].

policy comparable to the FTC's guidance on endorsements would provide authority for its local consumer protection agency to take action against Amazon for not only failing to ensure compliance but in fact for encouraging non-compliance. For Amazon to comply, it would need to apply its oversight over police departments just as zealously to ensure greater transparency about the effectiveness of its product, the benefits police departments are receiving for their endorsements of Ring and Neighbors, and the underlying partnership between Amazon and police departments more generally.

As anyone who has watched an advertisement replete with disclaimers can attest, such additional disclosures would likely chill consumer interest in the product, regardless of the content of those disclosures. Additionally, the content itself may cause political and cultural change in how citizens view their police departments and the individuals responsible for the policies of those departments, which in turn could result in a change in practices by those police departments in their dealings with vendors of surveillance products. These are admittedly indirect and hypothetical results. However, it may be the most immediately practical path forward in the absence of on-point federal privacy legislation.

In a best case scenario for privacy advocates, Amazon could be found liable for its own actions in addition to the actions of the police departments acting under its direction, stacking financial penalties for the multiple violations and potentially creating a stronger case for a broad injunction requiring greater transparency in advertising by Ring, including what it approves and/or pre-writes for police departments.

UDAP statutes presently provide states the ability to compel transparency in advertising, issue financial penalties for unsubstantiated claims used in advertising, and possibly even sue the offending government agencies (though that may not be politically feasible). Endorsement guidelines could provide a powerful tool for consumer protection agencies to attack tech giants routing sales through government entities using unfair or deceptive methods.

These approaches available through consumer protection law represent the fastest methods for creating friction in the otherwise explosive growth of surveillance technology directly *resulting from* unsavory partnerships between global tech companies and local police departments and likely *resulting in* disproportionate contact with the criminal justice system.

VI. CONCLUSION

Americans can expect inadequately disclosed partnerships between global technology companies and police departments to continue to proliferate in the absence of friction and deterrents making such partnerships inefficient. Although the most comprehensive solution would be a meaningful federal privacy law, a more immediate solution exists in consumer protection law. Although consumer privacy laws do not adequately address the underlying privacy issues of these technologies (especially their use by law enforcement), a more immediate solution that addresses transparency is

encouraged as the adoption of this technology continues to expand at a breakneck pace.