**NO. 15-16585**

---

**IN THE UNITED STATES COURT OF APPEALS**
**FOR THE NINTH CIRCUIT**

---

FEDERAL TRADE COMMISSION,
Plaintiff-Appellee,

v.

AT&T MOBILITY LLC,
Defendant-Appellant.

---

On Appeal from the United States District Court
For the Northern District of California
The Honorable Edward M. Chen, Presiding
United States District Court No. 3:14-cv-04785-EMC

---

# BRIEF OF *AMICI CURIAE* SOCIAL JUSTICE ORGANIZATIONS IN SUPPORT OF PLAINTIFF-APPELLEE FEDERAL TRADE COMMISSION'S PETITION FOR REHEARING *EN BANC*

---

Andrew Jay Schwartzman
Laura Moy
Institute for Public Representation
Georgetown University Law Center
600 New Jersey Avenue, NW
Suite 312
Washington, DC 20001
(202) 662-9535
*Counsel for Amici Curiae*

## CORPORATE DISCLOSURE STATEMENT

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, and Rule 29(c)(1) of the Rules of this Court, Color Of Change, The Center for Media Justice, and New America respectfully state that each of them is a non-profit organization with no parent companies, subsidiaries or affiliates and that none of them have issued shares to the public.

Respectfully submitted,

/s/ *Andrew Jay Schwartzman*

Andrew Jay Schwartzman
Institute for Public Representation
Georgetown University Law Center
600 New Jersey Avenue, NW
Suite 312
Washington, DC 20001
(202) 662-9535
*Counsel for Amici Curiae*

October 24, 2016

**STATEMENT OF COMPLIANCE WITH RULE 29(c)(5)**

No party's counsel authored the brief in whole or in part; no party or party's counsel contributed money that was intended to fund preparing or submitting the brief; and no person other than the *amici curiae*, their members, or their counsel, contributed money that was intended to fund preparing or submitting the brief.

Respectfully submitted,

/s/ *Andrew Jay Schwartzman*

Andrew Jay Schwartzman
Institute for Public Representation
Georgetown University Law Center
600 New Jersey Avenue, NW
Suite 312
Washington, DC 20001
(202) 662-9535
*Counsel for Amici Curiae*

October 24, 2016

## TABLE OF CONTENTS

CORPORATE DISCLOSURE STATEMENT ..... i

STATEMENT OF COMPLIANCE WITH RULE 29(c)(5) ..... ii

TABLE OF CONTENTS ..... iii

TABLE OF AUTHORITIES ..... iv

INTERESTS OF *AMICI CURIAE* ..... 1

SUMMARY OF ARGUMENT ..... 2

ARGUMENT ..... 4

I. The Panel Opinion Threatens the FTC's Ability to Protect Consumers from Unfair and Deceptive Data-Driven Activities ..... 4

II. The Panel Opinion Threatens the FTC's Ability to Protect Consumers from Data-Driven Activities that Disproportionately Harm Historically Disadvantaged Communities ..... 9

A. Part of the FTC's Exercise of Section 5 Authority Over Data-Driven Activities Is to Protect Against Disproportionate Harm to Historically Disadvantaged Communities ..... 10

B. The Panel Decision Could Hamstring the FTC's Ability to Protect Consumers from Data-Driven Harms that Fall Disproportionately on Historically Disadvantaged Communities ..... 14

CONCLUSION ..... 21

## TABLE OF AUTHORITIES

### Administrative Materials


Agreement Containing Consent Order, *In re Nomi Technologies*, FTC Docket No. C-4538 ..... 20

Complaint, *In re Nomi Technologies*, FTC Docket No. C-4538 ..... 19

Fed. Trade Comm'n, *Big Data: A Tool for Inclusion or Exclusion?* (2016) ..... 10, 11, 12, 13

Fed. Trade Comm'n, *Data Brokers: A Call for Transparency and Accountability* (2014) ..... 11

Fed. Trade Comm'n, *Internet of Things: Privacy and Security in a Connected World* (2015) ..... 8, 9

Fed. Trade Comm'n, *Privacy and Data Security Update (2014*) (Jan. 2015) ..... 7

Fed. Trade Comm'n, *Privacy and Data Security Update (2015*) (Jan. 2016) ..... 7

Fed. Trade Comm'n, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policy Makers* (2012) ..... 8

Order, *International Harvester Co.*, 104 Fed. Trade Comm'n 949, 1070 (1984) ..... 15


### Statutes


15 U.S.C. § 45(a) (2012) ..... 4, 6, 7, 8, 14, 15, 17, 19, 21


### Other Authorities


AdWords Help, *About Store Visit Conversions*, Google ..... 20

Amit Datta et al., *Automated Experiments on Ad Privacy Settings: A Tale of Opacity, Choice, and Discrimination* (Mar. 18, 2015) ..... 15

Bob Lord, *An Important Message About Yahoo User Security*, Yahoo! (Sept. 22, 2016) ..... 20

David Ingold and Spencer Soper, *Amazon Doesn't Consider the Race of Its Customers. Should It?*, Bloomberg (Apr. 21, 2016) ..... 17

Eugene Kim, *Amazon Has a Secret Plan to Replace FedEx and UPS Called 'Consume the City'*, Bus. Insider (Sept. 27, 2016) ..... 16

Exec. Office of the President, *Big Data: Seizing Opportunities, Preserving Values* 54 (2014) ..... 12
Latanya Sweeney, *Discrimination in Online Ad Delivery* (Jan. 28, 2013) ..... 15
Remarks of Jessica Rich, Director, Bureau of Consumer Protection, Fed. Trade Comm'n, Section 5 Symposium, *Built to Last: Section 5 and the Changing Marketplace* (Feb. 26, 2015) ..... 6
Spencer Soper, *Amazon to Bring Same-Day Delivery to Bronx, Chicago After Outcry*, Bloomberg (May 1, 2016) ..... 17
Valentino-Devries et al., *Websites Vary Prices, Deals Based on Users' Information*, Wall St. J. (Dec. 24, 2012) ..... 18

## INTERESTS OF *AMICI CURIAE*

*Amici curiae* are civil rights and social justice organizations that support the Federal Trade Commission's ("FTC") efforts to protect consumers from unfair and deceptive data-driven practices that disproportionately harm historically disadvantaged communities. *Amici* are very concerned that, by diminishing the FTC's Section 5 authority and creating an enforcement gap, the panel opinion could lead to an expansion of data-driven practices that harm communities of color and other historically disadvantaged communities.

The Center for Media Justice is a Black-led, multiracial, national, next-generation organization dedicated to achieving racial equity through communication rights, access, and representation.

Color Of Change is the nation's largest online racial justice organization, driven by over one million members. Color Of Change challenges decision-makers in corporations and government to create a more human and less hostile world for Black people in America.

New America's Open Technology Institute works at the intersection of technology and policy to ensure that every community has equitable access to digital technology and its benefits. It promotes universal access to communications technologies that are both open and secure.

## SUMMARY OF ARGUMENT

*Amici curiae*, The Center for Media Justice, Color Of Change, and New America's Open Technology Institute, file this brief to highlight the ways in which this case could undermine the federal government's ability to protect consumers from harms that flow from data-driven activities, including harms that disproportionately fall on historically disadvantaged communities. This is an issue of exceptional importance.

The FTC protects consumers from data-driven activities that are unfair and deceptive. In today's information economy, many companies collect, process, analyze, transfer, and apply consumer data to make decisions about or deliver services to consumers. These activities can be helpful to consumers, but they can also be harmful and unfair or deceptive.

The FTC recognizes the growing importance of and risks raised by data-driven activities and has in recent years used its Section 5 authority to engage with companies regarding questions of discriminatory impact. Indeed, the FTC has been shaping and facilitating public debate regarding the implications of unfair and deceptive data-driven practices for historically disadvantaged communities. And when necessary, the FTC has also taken enforcement action against companies engaging in such practices.

Some unfair and deceptive data-driven activities the FTC has worked to address are of particular interest to *amici* because they may disproportionately harm individuals in historically disadvantaged communities. For example, inaccuracies and biases in data or predictive algorithms can disproportionately affect particular communities. Certain communities are also disproportionately harmed when companies use data to target advertisements, misrepresent privacy policies, or fail to secure consumer data.

Under the panel's ruling, many companies engaging in these activities could arguably escape FTC Section 5 authority by establishing common carrier "status" with a common carrier service they already provide or a new service they could easily begin to provide. For example, companies like Google and Verizon are arguably now common carriers under the panel's erroneous opinion. Other companies, like Amazon and Staples, could quickly engage in practices that would bring them under the common carrier exception.

In today's information economy, companies from all corners of our economy must be monitored for potential missteps that could disproportionately affect historically disadvantaged communities. If allowed to stand, the panel's ruling would dramatically undermine the FTC's continuing oversight work.

To address this issue of exceptional importance, review by the *en banc* court is in order.

## ARGUMENT

The Federal Trade Commission has persuasively shown why the panel decision was wrongly decided and that it is in conflict with prior decisions of this Court and other circuits. *Amici* submit this brief to provide additional information as to why the FTC is also correct in stating that this case presents a matter of exceptional importance.

### I. The Panel Opinion Threatens the FTC's Ability to Protect Consumers from Unfair and Deceptive Data-Driven Activities

The panel opinion dramatically limits the FTC's ability to protect consumers from unfair or deceptive practices by invalidating the FTC's Section 5 authority over a large number of companies, even when they are engaged in non-common carrier activities.[1] This has a profound impact on the agency's jurisdiction because, as the FTC explains, "[m]any companies engage in both common carrier and non-common carrier activities."[2] This includes companies such as AT&T, Verizon, Comcast, Google, and DISH Network. It will also include companies that do not currently engage in common carrier activities, but are acquired by common carriers or decide to engage in such activities simply to take advantage of the now-broadened common carrier exception. *Amici* are

[1] 15 U.S.C. § 45(a) (2012).
[2] Fed. Trade Comm'n, Petition for Rehearing *En Banc* at 8.

particularly concerned by the implications of limiting the FTC's ability to police the many companies that engage in data-driven activities in the era of big data.

Consumers need a regulator with broad oversight of data-driven activities. As technology advances, the avenues for collection of consumer data are rapidly expanding both in number and in scope. Connected devices provide new opportunities for data collection: not only are laptops and smartphones equipped with computer chips and Internet connections, but so too are automobiles, toys, coffee makers, door locks, smoke detectors, and more. In addition, connected devices now collect unprecedented amounts of data from and about consumers. New and innovative apps also introduce new windows into consumers' private lives. The increased availability of consumer data creates new opportunities for companies to collect, analyze, and use these data sets.

The FTC is the natural agency to provide the broad oversight consumers need. It is the principal agency responsible for protecting consumers from unfair and deceptive practices, including new and unanticipated practices that arise as the information economy expands. In the FTC's own words, "no other federal agency has the FTC's breadth of authority to protect consumers from many

unfair or deceptive practices across the economy and to obtain redress for consumer harm."[3]

Where new technology and data-driven practices are concerned, the FTC uses its Section 5 enforcement authority to protect consumers against developing threats without impeding innovation. In the words of Jessica Rich, Director of the FTC's Bureau of Consumer Protection, Section 5 "is a workhorse for protecting consumers, deliberately designed by Congress to enable the FTC to address a wide range of practices in an ever-changing economy."[4] The FTC has used its deception authority to challenge false and misleading claims about how companies use and share consumer data, whether they track consumers' activities, whether they honor consumers' preferences, and whether they keep data secure.[5] It has used its unfairness authority to challenge harms flowing from data breaches, from the knowing sale of financial account data to scam artists, and from the use of software to surreptitiously capture consumers' sensitive data, location, and even photos of them in their homes.[6]

---

[3] *Id.* at 7-8.
[4] Remarks of Jessica Rich, Director, Bureau of Consumer Protection, Fed. Trade Comm'n, Section 5 Symposium, *Built to Last: Section 5 and the Changing Marketplace* 2 (Feb. 26, 2015), https://www.ftc.gov/system/files/documents/public_statements/626841/150226section5symposium.pdf.
[5] *Id.* at 4.
[6] *Id.*

Even when it is not bringing enforcement actions under Section 5, the FTC fosters public dialogue around policy questions that arise out of technological developments. The FTC has hosted over 35 workshops, town halls, and roundtables since 1996 to discuss emerging issues, such as Internet of Things (IoT), big data, and cross-device tracking.[7] The FTC has also authored over 50 reports from independent research or workshop discussions, including a report on mobile shopping apps and a study on credit report accuracy.[8] Moreover, the FTC provides educational materials for both consumers and businesses on a variety of privacy and data security issues, including identity theft, Internet safety for children, credit reporting, and behavioral advertising.[9]

The panel opinion jeopardizes the FTC's enforcement authority. As the FTC explains, it "has repeatedly enforced the FTC Act against the non-common-carriage activities of companies that also provide common carriage," and in so doing has recovered hundreds of millions of dollars for injured consumers.[10] If the panel opinion stands, the FTC may no longer be able to bring these cases.

---

[7] Fed. Trade Comm'n, *Privacy and Data Security Update (2015*) (Jan. 2016), https://www.ftc.gov/reports/privacy-data-security-update-2015; Fed. Trade Comm'n, *Privacy and Data Security Update (2014*) (Jan. 2015), https://www.ftc.gov/reports/privacy-data-security-update-2014.
[8] *Privacy and Data Security Update (2014)*, *supra* note 7.
[9] *Privacy and Data Security Update (2015)*, *supra* note 7.
[10] Petition for Rehearing *En Banc*, *supra* note 2, at 6.

Restrictions on the FTC's enforcement power will also undermine the agency's efforts to guide companies toward better consumer protection practices. For instance, the FTC's 2012 privacy report, relying in part on the Commission's Section 5 authority, encourages companies to incorporate effective data privacy practices into every aspect of their operations, simplify consumer privacy choices, and provide greater transparency about their privacy practices.[11] Each of these, when implemented by businesses, provides a foundation for the FTC to oversee and take enforcement action against companies that are not living up to promised or basic privacy standards.[12] Similarly, the FTC held a workshop in 2013 and subsequently released a report discussing the risks and benefits of IoT devices and recommending companies ensure that their devices have a reasonable level of built-in security, minimize the amount of data collected, and provide consumers with notice and choice about data collection practices.[13] Indeed, the FTC has flexed its oversight muscle

---

[11] *See generally* Fed. Trade Comm'n, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policy Makers* (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[12] The FTC has, in fact, taken such enforcement action, as described in Section II(A), *infra*.

[13] *See generally* Fed. Trade Comm'n, *Internet of Things: Privacy and Security in a Connected World* (2015), https://www.ftc.gov/system/files/documents/

against companies that have violated these principles in the past,[14] and the report suggests that if IoT device creators fail to follow these principles, the FTC will take enforcement action in the future.[15] However, if the panel opinion stands, companies with common carrier status will no longer be subject to the prohibition against unfair or deceptive practices, and will no longer have any reason to cooperate with the agency in protecting consumers.

## II. The Panel Opinion Threatens the FTC's Ability to Protect Consumers from Data-Driven Activities that Disproportionately Harm Historically Disadvantaged Communities

The panel opinion not only generally threatens consumer protections from unfair and deceptive data-driven activities, it specifically threatens consumer protections from data-driven activities that disproportionately harm historically disadvantaged communities. The FTC facilitates important public dialogue around innovative uses of data and has used its enforcement authority to stop discriminatory use of consumer data by companies. However, under the panel decision, many of these companies could fall under the common carrier exception.

---

reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

[14] *See generally id.*

[15] *See, e.g.*, *id.* at 30.

### A. Part of the FTC's Exercise of Section 5 Authority Over Data-Driven Activities Is to Protect Against Disproportionate Harm to Historically Disadvantaged Communities

The FTC monitors the collection and use of consumer data and works to protect consumers against uses that could cause unfair disproportionate harm to historically disadvantaged communities. The proliferation of data in today's economy has empowered companies across all sectors to analyze and interpret data to make predictions about consumer behavior. Data analytics can benefit historically disadvantaged communities by providing specialized healthcare or increasing employment opportunities, but can also cause disproportionate harm by excluding or selectively disadvantaging certain communities from benefits offered to others.[16] Future innovations may exacerbate this problem. To address the risks of data analytics, the FTC has initiated and cultivated important conversations around innovative uses of data. The FTC has also used its enforcement authority to stop discriminatory use of consumer data by companies.

[16] Fed. Trade Comm'n, *Big Data: A Tool for Inclusion or Exclusion?* i (2016), https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf [hereinafter Big Data Report].

The FTC is on the cutting edge of understanding the risks of discrimination and disparity to certain communities that result from data-driven activities. In 2014, the FTC released a report on companies that collect and sell consumers' personal information, known as data brokers, to shed light on an industry and practices of which many consumers are unaware.[17] The same year, the FTC hosted a public workshop to discuss the impact of big data on low-income and underserved populations and summarized the discussions in a report released in 2016.[18] The findings in the report highlight how companies could misuse data to discriminate against these populations.[19]

Data analytics may lead to discriminatory harm. One type of such harm may be caused by biases and errors in the underlying data itself.[20] Predictive analytics can be especially problematic when data sets are inaccurate, incomplete, or unrepresentative of the population.[21] This happens because some people are more careful about revealing their information, have unequal access

---

[17] Fed. Trade Comm'n, *Data Brokers: A Call for Transparency and Accountability* i (2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.
[18] *See generally* Big Data Report, *supra* note 16.
[19] *See generally id.*
[20] *Id.* at 20.
[21] *Id.*

to or less fluency with technology, or whose behaviors are not observed because they are not believed to be profitable constituencies.[22] Hidden and uncorrected biases in consumer data can also lead to incorrect predictions. These biases can develop, for example, when algorithms learn from human behavior and thereby incorporate human biases.[23] Furthermore, when large data sets are being analyzed, correlations become more readily identifiable, but analysts may incorrectly infer causation that can lead to discrimination.[24] For example, analysts could use this faulty process to create inaccurate consumer profiles, whereby they conclude that all people with a specific set of qualities behave in a certain way.[25] Using these profiles, they could make decisions about how to treat all people who fit that profile, even if they were not part of the original data set. Moreover, with analysis of large data sets, the discrimination and its source can be more difficult to detect and correct.[26] Finally, if a data set is large enough, even consumer information that was originally anonymous can be pieced together with other data sets to deanonymize the information.[27]

---

[22] *Id.* at 27.
[23] *Id.* at 28.
[24] *Id.* at 21.
[25] *See generally id.* at 29-31.
[26] *Id.* at 21.
[27] *See* Exec. Office of the President, *Big Data: Seizing Opportunities, Preserving Values* 54 (2014), https://www.whitehouse.gov/sites/default/files/

The ways in which companies use data can also disproportionately harm historically disadvantaged communities. These communities could be disproportionately harmed when companies decide not to target advertisements to some consumers because the data erroneously suggests they would not be eligible or have the resources for the particular product or service.[28] There may also be disproportionate harm when companies use data to engage in price discrimination.[29] Furthermore, companies can cause disproportionate harm by selling data to buyers that will use the data for discriminatory purposes.[30] Such disproportionate harm could also be caused when companies misrepresent their data privacy practices to consumers.[31] Finally, a company can cause disproportionate harm by failing to reasonably secure consumer data it holds or failing to ensure the products it sells to consumers have adequate security, thereby exposing consumers' personal and sensitive information, such as social security numbers or medical information.[32] In that last case, the data may have

---

docs/big_data_privacy_report_may_1_2014.pdf (explaining that, once collected, it can be difficult to keep data anonymous because there are advanced efforts to re-identify anonymous data with large data sets).

[28] Big Data Report, *supra* note 16, at 10.

[29] *Id.* at 11.

[30] *Id.* at 23.

[31] *Id.* at 21-22.

[32] *Id.* at 22.

inherent biases that cannot be controlled for because the source is obscure and when combined with other data sets can result in biased predictive analytics.

### B. The Panel Decision Could Hamstring the FTC's Ability to Protect Consumers from Data-Driven Harms that Fall Disproportionately on Historically Disadvantaged Communities

The panel decision's narrowing of FTC jurisdiction will have an actual negative impact on the FTC's ability to police data-driven activities that are found to be discriminatory or unfairly inflict disparate harm on certain segments of society. The FTC has used its Section 5 authority to take enforcement action against a number of companies whose data-driven activities have resulted in such harm. Other companies may have avoided those same violative practices because the FTC's enforcement power and activity serve as an effective deterrent. Some of these companies engage in common-carrier activities and may now have common carrier status and fall under the exception. Others are already exploring common carrier activities or stand as prime candidates to begin doing so—activities that could enable them to escape FTC jurisdiction under the panel opinion's interpretation of the common carrier exception.

The panel opinion threatens the FTC's jurisdiction over companies that arguably have common carrier status, but that use consumer data outside of the common carrier context in a way that could have a discriminatory or disparate

impact on persons of a certain race or gender. Google, which operates Google Fiber and also is the industry leader in online advertising, is such a company. And there are important reasons for regulators to monitor Google's activities for potential race- and gender-specific harms. Google searches of names traditionally associated with Black people have resulted in ads suggestive of a criminal record at a higher rate than searches of non-Black names.[33] On employment-related websites, ads served up by Google offered career coaching service for high-paying jobs more often to men than to women.[34] The disparate presentation of ads is almost certainly not intentional on Google's part, but rather a reflection of poorly designed ad targeting algorithms that fail to anticipate such problems. Nevertheless, this could be considered unfair under Section 5 because racially disparate presentation of ads could negatively affect employment opportunities on a class-wide basis.[35] The panel decision could reduce the FTC's authority to protect consumers from Google's targeted ads

---

[33] Latanya Sweeney, *Discrimination in Online Ad Delivery* (Jan. 28, 2013), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2208240.

[34] Amit Datta et al., *Automated Experiments on Ad Privacy Settings: A Tale of Opacity, Choice, and Discrimination* 13, 21 (Mar. 18, 2015), https://www.andrew.cmu.edu/user/danupam/dtd-pets15.pdf.

[35] The FTC requires three elements to be met for consumer injury to be unfair: (1) it must be substantial; (2) it must not be outweighed by any countervailing benefits to consumers or competition produced by the practice; and (3) it must be an injury that consumers could not reasonably have avoided. Order, *International Harvester Co.*, 104 Fed. Trade Comm'n 949, 1070 (1984).

because the entirety of the Google enterprise could claim common carrier status simply because its Google Fiber division provides broadband service, and is therefore a common carrier.

The panel opinion could also negatively affect the FTC's jurisdiction over companies that are starting to adopt common carrier activities and have previously changed discriminatory practices under threat of FTC action. For example, Amazon could escape FTC jurisdiction over unfair data-driven practices by achieving common carrier status.[36] This would be problematic for consumers because Amazon engages in innovative uses of consumer data that could harm consumers on a racially disparate basis, and that therefore unfair or deceptive data-driven practices. For example, an investigation by Bloomberg revealed that Amazon has been offering free same-day delivery service to its "Prime" members in certain neighborhoods with a high rate of Prime use. Investigation revealed, though, that the free same-day service was being made available to Prime members in predominately White neighborhoods while

[36] This is not a far-fetched idea. Amazon is steadily moving in the direction of providing package delivery, not just for the retail goods it sells, but also to ship other customers' packages, FedEx and UPS. Eugene Kim, *Amazon Has a Secret Plan to Replace FedEx and UPS Called 'Consume the City'*, Bus. Insider (Sept. 27, 2016), http:// www.businessinsider.com/amazon-secret-plan-replace-fedex-ups-called-consume-the-city-2016-9. In that case, Amazon, like other package delivery providers, could claim common carrier status.

excluding predominately Black neighborhoods.[37] For example, in Boston, three ZIP codes that include predominately Black neighborhoods were not eligible for free same-day delivery service, even though surrounding neighborhoods within a 15-minute walking distance qualified for same-day delivery.[38] As with Google, this problem was almost certainly accidental, flowing from the fact that Amazon Prime is used more heavily on average by Whites than by Blacks.[39] In response to public outcry that included U.S. Representative Bobby Rush calling for an FTC investigation, Amazon agreed to extend its same-day delivery service to many of the neighborhoods that had not been eligible for the service.[40] However, the threat of FTC investigation would no longer exist if companies like Amazon could escape FTC Section 5 oversight by establishing common carrier status.

In addition, the benefit of escaping FTC Section 5 oversight could create a perverse incentive for companies that have no plans to engage in common carrier activities to alter their course and attempt to achieve common carrier

---

[37] David Ingold & Spencer Soper, *Amazon Doesn't Consider the Race of Its Customers. Should It?*, Bloomberg (Apr. 21, 2016), http://www.bloomberg.com/graphics/2016-amazon-same-day.
[38] *Id.*
[39] *Id.*
[40] Spencer Soper, *Amazon to Bring Same-Day Delivery to Bronx, Chicago After Outcry*, Bloomberg (May 1, 2016), https://www.bloomberg.com/news/articles/2016-05-01/amazon-pledges-to-bring-same-day-delivery-to-bronx-after-outcry.

status specifically for this purpose. Retailers engaging in price discrimination might have just such an incentive, yet price discrimination could unfairly harm consumers in a racially disparate way. For example, a 2012 Wall Street Journal investigation into Staples' online store discovered lower prices for customers whose ZIP code was located within 20 miles of a rival retailer's store.[41] ZIP codes where Staples charged discounted prices generally had higher weighted average income than the ZIP codes that were subject to higher prices.[42] The price difference may well have been an unintended result of Staples' pricing algorithms, but the use of geography as a pricing tool could reinforce existing disparities by resulting in higher prices for rural or poor areas where there is less competition.[43] This disparate harm could be considered unfair. If, however, Staples were to expand its business to the offering of prepaid cell phone plans or trucking retail products—not an impossible stretch—it could claim common carrier status in an attempt to escape FTC jurisdiction.

Smaller companies could be acquired by larger companies and escape future FTC oversight even when they have previously been subject to FTC

---

[41] Valentino-Devries et al., *Websites Vary Prices, Deals Based on Users' Information*, Wall St. J. (Dec. 24, 2012), http://www.wsj.com/articles/SB10001424127887323777204578189391813881534.
[42] *Id.*
[43] *Id.*

action for unfairly and deceptively not keeping promises to consumers about data usage, with discriminatory results. The FTC recently took Section 5 action against a company that tracks consumers while in retail stores. Nomi Technologies, Inc. uses mobile device tracking technology to provide analytics services to brick and mortar retailers.[44] These devices collect information about consumers from their phones—the dates and times when they visit a particular retailer, the amount of time they spend there, whether they return, and whether they visit another location in the chain.[45] Nomi aggregates and shares this information with retailers.[46] The data could be used to discriminate. For example, Nomi could sell the data to a data broker that draws conclusions about a particular consumer's shopping habits, such as if the consumer shops at high-end retailers. Conversely, the information could be used to conclude that a consumer is not a reliable high-cost buyer. In either case, the information could be used to target advertisements to some consumers and not others. In 2015, the FTC entered into a consent decree with the company regarding alleged deceptive conduct flowing from Nomi's failure to adhere to its own privacy

[44] Complaint at 1, *In re Nomi Technologies*, FTC Docket No. C-4538, https://www.ftc.gov/ system/files/documents/cases/150902nomitechcmpt.pdf.
[45] *Id.* at 1-2.
[46] *Id.* at 2.

policy.[47] But if a company with common carrier status were to acquire Nomi—for example, Google, which has taken steps to track consumer visits to brick and mortar stores[48]—the company's practice could fall outside the FTC's Section 5 authority in the future.

When one large company acquires another large company with weak data security practices, the resulting breach poses a risk of substantial harm to historically disadvantaged communities. In September 2016, Yahoo announced that information from at least 500 million user accounts was stolen by hackers in 2014.[49] Hacked account information included names, email addresses, telephone numbers, dates of birth, and in some cases, security questions and passwords.[50] By itself, this information can be grouped with existing data to deanonymize user information and create consumer profiles, which can be used in a discriminatory fashion. This information can also be used to access a user's many other online accounts, which contain even more sensitive information,

---

[47] Agreement Containing Consent Order at 1, *In re Nomi Technologies*, FTC Docket No. C-4538, https://www.ftc.gov/system/files/documents/cases/150423nomiorder.pdf.
[48] AdWords Help, *About Store Visit Conversions*, Google, https://support.google.com/adwords/answer/6100636?hl=en (last visited Oct. 24, 2016).
[49] *See* Bob Lord, *An Important Message About Yahoo User Security*, Yahoo! (Sept. 22, 2016), https://yahoo. tumblr.com/ post/150781911849/an-important-message-about-yahoo-user-security.
[50] *Id.*

such as credit ratings or medical histories. Yahoo's data security breach—one of the largest security breaches to date—could be a Section 5 violation by failing to maintain adequate and reasonable security measures to protect consumer privacy. However, under the panel decision Yahoo would fall under the exception from the FTC's jurisdiction once it finalizes its merger with Verizon, a common carrier, and leave 500 million consumers unprotected.

## CONCLUSION

For the reasons given above, and in the more comprehensive submission of the Federal Trade Commission, *amici curiae* respectfully urge that the panel decision be vacated, and that this Court order that the case be reheard *en banc*.

Respectfully submitted,

/s/ *Andrew Jay Schwartzman*

Andrew Jay Schwartzman
Laura Moy
Institute for Public Representation
Georgetown University Law Center
600 New Jersey Avenue, NW
Suite 312
Washington, DC 20001
(202) 662-9535
*Counsel for Amici Curiae*

October 24, 2016

## CERTIFICATE OF COMPLIANCE

I hereby certify that the foregoing brief complies with the typeface requirements of Federal Rule of Appellate Procedure 32(a)(5) and the type-style requirements of Federal Rule of Appellate Procedure 32(a)(6). The brief is composed in a 14-point proportional typeface, Times New Roman, and complies with the word limit of Federal Rule of Appellate Procedure 32(a)(7)(B) and Rule 29-2(c)(2) of the United States Court of Appeals for the Ninth Circuit because it contains 4,172 words, excluding the parts of the brief exempted under Federal Rule of Appellate Procedure 32(a)(7)(B)(iii).

Respectfully submitted,

/s/ *Andrew Jay Schwartzman*

Andrew Jay Schwartzman
Institute for Public Representation
Georgetown University Law Center
600 New Jersey Avenue, NW
Suite 312
Washington, DC 20001
(202) 662-9535
*Counsel for Amici Curiae*

October 24, 2016

## CERTIFICATE OF SERVICE

I hereby certify that, on October 24, 2016, I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit using the appellate CM/ECF system. Participants in the case who are registered CM/ECF users will be served by the appellate CM/ECF system.

/s/ *Andrew Jay Schwartzman*
Andrew Jay Schwartzman