

No. 18-956

In The
Supreme Court of the United States

— ♦ —
GOOGLE LLC,
Petitioner,

v.

ORACLE AMERICA, INC.,
Respondent.

— ♦ —
ON WRIT OF CERTIORARI TO
THE UNITED STATES COURT OF APPEALS
FOR THE FEDERAL CIRCUIT

— ♦ —
BRIEF OF USTELECOM – THE BROADBAND
ASSOCIATION AS *AMICUS CURIAE*
SUPPORTING RESPONDENT

Patrick R. Halley
Senior Vice President
Policy and Advocacy
USTELECOM – THE
BROADBAND ASSOCIATION
601 New Jersey Ave, NW
Suite 600
Washington, DC 20001
(202) 326-7300
phalley@ustelecom.org

Russell P. Hanser
Counsel of Record
Jennifer B. Tatel
Nicholas G. Alexander
WILKINSON BARKER
KNAUER, LLP
1800 M Street, NW
Suite 800N
Washington, DC 20036
(202) 783-4141
rhanser@wbklaw.com

Counsel for Amicus Curiae *Dated: February 19, 2020*

TABLE OF CONTENTS

	Page
STATEMENT OF INTEREST	1
INTRODUCTION AND SUMMARY OF ARGUMENT	2
ARGUMENT	5
I. USTELECOM’S MEMBERS ARE BUILDING NEXT-GENERATION NETWORKS THAT INCREASINGLY RELY ON SOFTWARE INTERFACES	5
A. USTelecom Members and Other Network Providers Have Invested Huge Sums of Money Into Their Networks, and Anticipate Investing Even More	6
B. Next-Generation Networks Increasingly Rely on Software	7
II. A HOLDING FAILING TO RECOGNIZE THE IMPORTANCE AND COPYRIGHTABILITY OF “SOFTWARE INTERFACES” WOULD UNDERMINE PROVIDERS’ ABILITY TO FULFILL KEY LEGAL AND BUSINESS OBLIGATIONS.....	10
A. USTelecom Members Must Ensure Network Security and Resilience.....	12

B. USTelecom Members Must Ensure Their Customers' Privacy	14
C. USTelecom Members Must Retain Flexibility to Innovate and Compete as New Business Models Arise	17
D. USTelecom Members Would Be Impeded in Achieving These Critical Goals if All Software Interface Were Ineligible for Copyright Protection	19
E. Alternative Means of Protecting Property Rights in Software Interfaces Are Less Effective or Less Practical Than Copyright.....	23
CONCLUSION	26

TABLE OF AUTHORITIES

	Page(s)
 CASES	
<i>Alice Corp. Pty. Ltd. v. CLS Bank Int’l</i> , 573 U.S. 208 (2014).....	24, 25
<i>Feist Publ’ns, Inc. v. Rural Tel. Serv. Co.</i> , 499 U.S. 340 (1991).....	24
 CONSTITUTIONAL PROVISION	
U.S. CONST. Art. 1, Sec. 8, Cl. 8.....	2
 STATUTES	
15 U.S.C. § 45.....	16
15 U.S.C. § 45(a)(1).....	16
17 U.S.C. § 102(a)	24
35 U.S.C. § 101.....	24
35 U.S.C. § 103.....	24
47 U.S.C. § 151.....	13
47 U.S.C. § 222.....	15
47 U.S.C. § 338(i)	16
47 U.S.C. § 551.....	16

Cal. Civ. Code §§ 1798.100-1798.199.....	17
--	----

RULE

Sup. Ct. R. 37.6.....	1
-----------------------	---

REGULATIONS

47 C.F.R. Part 4	13
47 C.F.R. § 15.31(a)(4)	22
47 C.F.R. § 64.2001 <i>et seq.</i>	15
47 C.F.R. § 64.2009(b)	16
47 C.F.R. § 64.2009(c).....	16
47 C.F.R. § 64.2010(a)	16
47 C.F.R. § 79.103(c)(11)	22

OTHER AUTHORITIES

<i>Charter of the FCC’s Communications Security, Reliability, and Interoperability Council, Section 3</i> (Mar. 19, 2017), https://www.fcc.gov/file/12251/download	14
--	----

Cisco, <i>Reimagining the End-to-End Mobile Network in the 5G Era</i> (2019), https://www.cisco.com/c/dam/en/us/products/collateral/cloud-systems-management/elastic-services-controller-esc/reimagining-mobile-network-white-paper.pdf	9
--	---

Comments of CTIA before the Federal Communications Commission, GN Docket No. 19-285, at 3 (filed Nov. 22, 2019), https://ecfsapi.fcc.gov/file/112291564913/191122%20CTIA%20Section%20706%20Comments%20-%20FINAL.pdf	7
Comments of NCTA – The Internet & Television Association before the Federal Communications Commission, GN Docket No. 17-142, at 1 (filed Aug. 30, 2019), https://ecfsapi.fcc.gov/file/1083002214668/08302019%2017-142%20NCTA%20MTE%20Comments.pdf	7
Dan Littmann, Kieran Norton, & Ajit Prabhu, <i>Connectivity of tomorrow, The spectrum and potential of advanced networking</i> , Deloitte (Jan. 16, 2019), https://www2.deloitte.com/us/en/insights/focus/tech-trends/2019/future-of-connectivity-advanced-networking.html	8
Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, <i>National Critical Functions: An Evolved Lens For Critical Infrastructure Security and Resilience</i> 1, 3 (Apr. 30, 2019), https://www.cisa.gov/sites/default/files/publications/national-critical-functions-overview-508.pdf	13
Department of Homeland Security, <i>Communications Sector-Specific Plan, An Annex to the NIPP 2013</i> (2015) (2013 NIPP Annex), https://www.cisa.gov/sites/default/files/publications/nipp-ssp-communications-2015-508.pdf	13

Federal Communications Commission, Network Outage Reporting System (NORS), https://www.fcc.gov/network-outage-reporting-system-nors (last updated July 5, 2018).....	13
Federal Communications Commission, Voice Telephone Services: Status as of December 31, 2017 2 (Aug. 2019).....	18
Federal Trade Commission, Privacy & Data Security Update: 2018, January 2018 - December 2018 (rel. Mar. 15, 2019), https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2018/2018-privacy-data-security-report-508.pdf	16
Federal Trade Commission, Privacy and Security Enforcement, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited Feb. 18, 2020).....	17
Fenwick & Alice LLP, Decoding Patent Eligibility Post- <i>Alice</i> Patent Eligibility Case Analysis Tool, https://www.fenwick.com/pages/post-alice.aspx (last visited Feb. 18, 2020)	25
<i>Inquiry Concerning Deployment of Advanced Telecommunications Capability to All Americans in a Reasonable and Timely Fashion</i> , Fifteenth Broadband Deployment Report Notice of Inquiry, 34 FCC Red 10092, 10093 ¶ 3 (2019).....	7

Kate Gaudry & Samuel Hayim, <i>Years After Alice: Eligibility-Rejections Outflow from a Different Part of the USPTO</i> , JDSupra (Mar. 5, 2019), https://www.jdsupra.com/legalnews/years-after-alice-eligibility-70833/	25
<i>Nat'l Comm'n on New Tech. Uses of Copyrighted Works</i> , Final Report, III.C.1.c (1979), https://files.eric.ed.gov/fulltext/ED160122.pdf	21
<i>New Part 4 of the Commission's Rules Concerning Disruptions to Communications</i> , Report and Order and Further Notice of Proposed Rulemaking, 19 FCC Rcd 16830, 16833 ¶ 1 (2004) (adopting 47 C.F.R. Part 4)	14
Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (1996)	17
United States Copyright Office, Copyright Office Fees, Circular 4 at 7-8 (Apr. 2018), https://www.copyright.gov/circs/circ04.pdf	24
USTelecom, <i>USTelecom Industry Metrics and Trends 2020</i> 13, 27 (Feb. 2020) (USTelecom Industry Metrics), https://www.ustelecom.org/wp-content/uploads/2020/02/USTelecom-State-of-Industry-2020.pdf	6
USTelecom, <i>USTelecom Issue Brief, Digital Privacy</i> (Apr. 2019), https://www.ustelecom.org/wp-content/uploads/2019/04/USTelecom-Brief-Privacy-4.19.pdf	15

*Verizon; Compliance with the Commission's Rules
and Regulations Governing Customer Proprietary
Network Information, Adopting Order, 29 FCC Red
10303 (Enforcement Bureau 2014) 16*

STATEMENT OF INTEREST¹

USTelecom – The Broadband Association (USTelecom) respectfully submits this brief as *amicus curiae*.

USTelecom is the premier trade association representing service providers and suppliers for the telecommunications industry. USTelecom’s member companies offer a wide range of services across communications platforms, including voice, video, and data provisioned over local exchange, long distance, wireless, internet, and cable networks. These companies range from large, publicly traded companies to small rural cooperatives, touching every corner of the United States. USTelecom advocates on behalf of its members before Congress, regulators, and the courts for policies that will enhance the economy and facilitate a robust telecommunications industry.

USTelecom has a substantial interest in the outcome of this appeal because the position advanced by Petitioner has the potential to eliminate copyright as a tool available to network providers, limiting their ability to ensure security and resiliency, to protect customer privacy, and to maintain the ability to innovate and compete.

¹ Pursuant to Supreme Court Rule 37.6, counsel for *amicus curiae* represent that they authored this brief in its entirety and that no party or counsel for a party, other than *amicus curiae*, its members, or its counsel, made any monetary contribution to fund the preparation or submission of this brief. The parties have consented to the filing of this brief.

INTRODUCTION AND SUMMARY OF ARGUMENT²

Petitioner Google LLC argues that software interfaces – a term it broadly defines as “a means of connecting to, interacting with, or operating computer software” – are ineligible for copyright protection under the judicially created merger doctrine. If accepted, Petitioner’s position could result in harms to telecommunications providers and their consumers. It also could frustrate innovation and impede the progress of science and useful arts, the promotion of which, after all, is the whole purpose of copyright law. U.S. Const. Art. 1, Sec. 8, Cl. 8. USTelecom therefore urges this Court to consider carefully the potential harms to software-driven next-generation communications networks and the software-driven services and applications riding over those networks that would arise if software interfaces were ineligible for copyright, even when they otherwise met the applicable criteria for such protection.

USTelecom’s members offer a wide range of services across communications platforms, including voice, video, and data provisioned over local exchange, long distance, wireless, internet, and cable networks. They have invested many billions of dollars to construct ever-expanding and ever-improving networks. Other providers, including but not limited to wireless carriers (some but not all of which are USTelecom members), cable companies, and satellite operators,

² The views stated herein do not reflect the views of all USTelecom members, including Verizon and CenturyLink, who take no position before this court on the issues raised herein or the matters presented in the underlying case.

have invested billions more. As competition becomes increasingly intense, providers of all stripes continue to invest, attempting to differentiate their services and attract consumers.

The current generation of networks differ from prior iterations in significant ways. Perhaps most importantly, these networks use software and software interfaces to perform functions that were in the past performed by hardware. For example, capabilities that allow providers to route traffic were once hard-wired into networks, but are migrating – or have migrated – to software loaded onto network components. The rise of software-defined networks affords providers far more flexibility than they enjoyed before. Where once a communications provider might need to replace physical equipment across its network to effectuate updates or repairs, now it often can simply push new software to its network components, using the network itself to do so. This network “virtualization” also lets providers craft unique services customized to a particular customer’s needs. Software-defined networks are thus both less expensive and more useful than their predecessors.

Given the rise of software-defined networks, Petitioner’s contention that software interfaces cannot be copyrighted could seriously harm USTelecom’s members, other providers, consumers, and the public interest. Communications companies are subject to a raft of legal, contractual, and competitive imperatives, and their ability to fulfill these objectives would be undermined if they and their vendors were unable to copyright the relevant software. For example, USTelecom’s members must maintain the security

and resiliency of their networks, which have been deemed critical infrastructure. Likewise, communications providers are subject to a web of laws and regulations requiring that they protect users' privacy. Further, competitive dynamics require that telecommunications providers remain able to innovate, developing new capabilities that match consumers' evolving needs.

These objectives could be thwarted if Petitioner's view of copyright prevailed. Loss of the ability to guard from appropriation the software at the heart of their networks would eviscerate providers' ability to ensure security and resiliency, to protect customer privacy, and to innovate and compete. Other types of protection do not play the role played by copyright. Communications providers must share access to their code in order to facilitate network interconnection, which is needed to allow the exchange of traffic between and among competing networks. Such sharing, however, could endanger protection under the trade secret doctrine. Likewise, patent law protects a far narrower class of intellectual property than copyright, and the process of obtaining a patent is long and cumbersome in comparison to the copyright process. Finally, protections grounded in state tort or contract law would subject providers to protracted state-by-state litigation, culminating in a patchwork quilt of protections, in which the software at the root of their networks might be protected in some states but not in others.

In short, telecommunications providers must retain the ability to copyright the software implementing their network interfaces. The loss of this protection would imperil their ability to comply with legal obligations and market imperatives alike, harming consumers and the broader public.

ARGUMENT

I. USTELECOM'S MEMBERS ARE BUILDING NEXT-GENERATION NETWORKS THAT INCREASINGLY RELY ON SOFTWARE INTERFACES

USTelecom is a trade association whose members provide a wide range of communications offerings to consumers across the United States. Those members have invested billions upon billions of dollars constructing advanced networks designed to meet consumers' ever-changing needs. They expect and intend to continue making such investments. The next-generation of fixed and wireless networks will differ from past generations in important ways. Most notably, the networks of the future will increasingly rely on software that runs on commercial off-the-shelf (COTS) hardware to perform functions that were once embedded into specialized, proprietary network hardware. This move will confer numerous benefits – among other things, the shift to software will enable providers to more easily update and upgrade their networks without costly and time-consuming hardware upgrades or replacements.

A. USTelecom Members and Other Network Providers Have Invested Huge Sums of Money Into Their Networks, and Anticipate Investing Even More

Telecommunications companies have a long history of large capital expenditures. USTelecom expects this trend to continue.

Between 1996 (when Congress adopted the Telecommunications Act of 1996, described below) and 2018, communications providers of all varieties invested more than \$1.7 trillion in capital into their networks – \$387.2 billion of which came during the last five years of that window.³ Because of these efforts from industry, the United States has been a world leader in broadband investment. From 2003 to 2015, U.S. broadband providers invested \$245 per capita – more than 1.5 times as much as the \$151 average for Organization for Economic Cooperation and Development countries.⁴

These massive economic contributions are not solely attributable to USTelecom’s membership. Cable providers have invested more than \$290 billion in

³ USTelecom, *USTelecom Industry Metrics and Trends 2020* 13, 27 (Feb. 2020) (USTelecom Industry Metrics), <https://www.ustelecom.org/wp-content/uploads/2020/02/USTelecom-State-of-Industry-2020.pdf>.

⁴ *Id.* at 29-30.

the last 20 years to deploy broadband networks,⁵ and the wireless industry (which includes several USTelecom members but also many other providers) invested more than \$27 billion in 2018 alone.⁶ The latest figures from the Federal Communications Commission (FCC), published in 2019, show “broadband investment . . . up [year-over-year] more than \$1.5 billion, while fiber networks passed 5.9 million new homes, the largest single-year increase ever.”⁷

B. Next-Generation Networks Increasingly Rely on Software

As USTelecom’s members and other communications providers invest in expanding and enhancing their networks, they are engaged in a historic pivot. For much of the past, the “intelligence” of telecommunications networks was embedded in their physical components – i.e., their “hardware.” The instructions enabling the network to direct traffic from one user to another resided within complex, purpose-specific network hardware, including “switches” and “routers,” as did capabilities ranging from the ability to change the

⁵ Comments of NCTA – The Internet & Television Association before the Federal Communications Commission, GN Docket No. 17-142, at 1 (filed Aug. 30, 2019), <https://ecfsapi.fcc.gov/file/1083002214668/08302019%2017-142%20NCTA%20MTE%20Comments.pdf>.

⁶ Comments of CTIA before the Federal Communications Commission, GN Docket No. 19-285, at 3 (filed Nov. 22, 2019), <https://ecfsapi.fcc.gov/file/112291564913/191122%20CTIA%20Section%20706%20Comments%20-%20FINAL.pdf>.

⁷ *Inquiry Concerning Deployment of Advanced Telecommunications Capability to All Americans in a Reasonable and Timely Fashion*, Fifteenth Broadband Deployment Report Notice of Inquiry, 34 FCC Rcd 10092, 10093 ¶ 3 (2019) (footnote omitted).

bandwidth of an enterprise customer’s data connection, interrupt an ongoing call to announce another incoming communications (call waiting), to the features ensuring that 911 calls were routed to appropriate “public safety answering points.” Hardware-based intelligence worked well for decades, but also suffered from various drawbacks. For example, improvements to existing capabilities, or the addition of new capabilities, typically required physical upgrades to, or even replacement of, each individual piece of hardware in the network – often dozens, or even hundreds of pieces of equipment. Moreover, because intelligence resided in hardware, the same “instructions” applied to all traffic traversing any particular network component, sharply limiting a provider’s ability to offer specialized capabilities to different customers or make rapid changes or upgrades to a customer’s existing services.

In response to these limitations, numerous functions traditionally performed by hardware are increasingly being “virtualized” and performed by software running on generic, COTS hardware, birthing an era of software-defined networks (SDNs). An SDN “is a software layer” that operates on the network hardware and “can centrally program and manage [the] network.”⁸ In an SDN, functions traditionally built into hardware, including routing, switching, en-

⁸ Dan Littmann, Kieran Norton, & Ajit Prabhu, *Connectivity of tomorrow, the spectrum and potential of advanced networking*, Deloitte (Jan. 16, 2019), <https://www2.deloitte.com/us/en/insights/focus/tech-trends/2019/future-of-connectivity-advanced-networking.html>.

encryption, and security, are instead performed via software.⁹ SDNs “raise[] the bar on network flexibility, making it possible to configure networks to fit different types of . . . requirements” and allowing providers “to dynamically configure and control network resources through software.”¹⁰ Whereas network providers once would need to individually upgrade or replace expensive equipment in order to install new features or remedy problems, they can modify, upgrade, and repair their SDNs simply by installing new versions of relevant software, using the network itself to deliver and install the fix. Moreover, SDNs allow providers to more easily offer tailored network capabilities that meet the needs of individual customers, facilitating a user experience customized to a degree never before possible. The move to SDNs also ushers in a new age of modular competition within the network, in which communications providers can choose among a range of software packages developed by different vendors, each of which might offer unique capabilities, and from a broader universe of hardware manufacturers.¹¹

The ongoing migration toward SDNs lies at the root of USTelecom’s interest in this litigation, because SDNs utilize – indeed, could not function without – “software interfaces,” at least as Petitioner Google de-

⁹ *See ibid.*

¹⁰ *Ibid.*

¹¹ *See generally* Cisco, *Reimagining the End-to-End Mobile Network in the 5G Era* (2019), <https://www.cisco.com/c/dam/en/us/products/collateral/cloud-systems-management/elastic-services-controller-esc/reimagining-mobile-network-white-paper.pdf>.

finer that term. Specifically, Petitioner defines “software interface” as “a means of connecting to, interacting with, or operating computer software.” Br. of the Petitioner at 5 n.2 (filed Jan. 6, 2020) (Pet. Br.). Petitioner contends that there can be no copyright in such software interfaces. If Petitioner prevailed here, USTelecom’s members, other communications providers, and third-party developers would find themselves unable to assert property rights over their network interfaces – interfaces that for more than 100 years have resided in the hardware that they have indisputably owned and controlled. For reasons detailed below, this result would undermine providers’ ability to fulfill their obligations under the law and to their customers, harming the public interest.

II. A HOLDING FAILING TO RECOGNIZE THE IMPORTANCE AND COPYRIGHTABILITY OF “SOFTWARE INTERFACES” WOULD UNDERMINE PROVIDERS’ ABILITY TO FULFILL KEY LEGAL AND BUSINESS OBLIGATIONS

USTelecom’s members and other communications providers participate in an industry that is essential to the nation’s economy, national security, and public safety. The industry is pervasively regulated and highly competitive, and providers are subject to a wealth of overlapping legal obligations, contractual requirements, and market forces. As operators of critical infrastructure, they must comply with a range of obligations designed to ensure that their networks are secure and resilient to threat. As stewards of their consumers’ sensitive commercial and personal infor-

mation, they must protect their users' sensitive commercial data and personally identifiable information, and are subject to a web of mandates, overseen by the FCC, the Federal Trade Commission (FTC), the Department of Justice, and the states, designed to ensure that they do so. As players in an intensely competitive marketplace, they must constantly innovate to meet fast-evolving customer demands. Yet the very nature of the telecommunications industry also requires that network providers cooperate to ensure that their networks are interconnected and interoperable so that all users can communicate with one another, irrespective of which provider they rely upon for service. To facilitate such interconnection, providers must share details regarding their interfaces – interfaces that, as noted above, are quickly migrating from network hardware to software. This puts USTelecom's members in a bind: They must collaborate with competitors by sharing information regarding software-based interfaces, but must also retain control over the code developed to implement those interfaces, for a loss of such control would undercut their ability to ensure network security, to protect user privacy, and to develop innovative offerings that will allow them to succeed in the competitive marketplace.

Copyright provides the protection that these providers require. Unlike trade secret protection, copyright allows the rights-holder to share code without surrendering its rights.

Unlike patents, copyrights afford protection to the expressions of a process or method, allowing for numerous variations, whereas patent protects the

processes and methods themselves. Also, unlike patents, copyrights can be obtained via relatively simple processes. And unlike contract and tort law, copyright offers a uniform national framework that does not raise the specter of state-by-state litigation and disparate decisions in different jurisdictions.

If adopted here, Petitioner’s argument that “software interfaces” can *never* be copyrighted would deprive telecommunications providers of a tool to protect their rights in the contemporary marketplace – a marketplace in which functions are increasingly performed by software, in which competitors must be given access to software interfaces, and in which a provider’s loss of control over the software code implementing those interfaces would prevent it from fulfilling its legal obligations and effectively competing for customers.

A. USTelecom Members Must Ensure Network Security and Resilience

USTelecom members operate the high-speed broadband networks that carry voice, video, and data communications between and among American consumers, businesses, hospitals, governmental agencies, and military installations. In light of their importance to all aspects of the nation’s political, economic, and civic life, the Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency has identified these communications networks as “critical infrastructure” that is “so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public

health or safety, or any combination thereof.”¹² Members of the public rely on these networks to reach first responders when there’s an emergency, businesses use them to host and run critical applications, and national security agencies use them to safeguard us from threats both foreign and domestic. Indeed, Congress created the FCC, the primary regulator of communications providers such as USTelecom’s members, for the very purpose of ensuring that communications networks would be available to promote the “safety of life and property” and “the national defense.” 47 U.S.C. § 151.

In light of the above, USTelecom’s members must ensure the security and resiliency of their networks – both as a legal matter and as a business imperative. They must, for example, file mandatory network outage notifications with the FCC generally within 30 minutes of determining that a network problem has caused a significant degradation in the ability of an end user to establish and maintain communications.¹³ This obligation, in the FCC’s words, reflects the fact that such service disruptions “could affect homeland security, public health or safety, and

¹² Dep’t of Homeland Security, Cybersecurity and Infrastructure Security Agency, *National Critical Functions: An Evolved Lens For Critical Infrastructure Security and Resilience* 1, 3 (Apr. 30, 2019), <https://www.cisa.gov/sites/default/files/publications/national-critical-functions-overview-508.pdf>; Dep’t of Homeland Security, *Communications Sector-Specific Plan, An Annex to the NIPP 2013* (2015) (2013 NIPP Annex), <https://www.cisa.gov/sites/default/files/publications/nipp-ssp-communications-2015-508.pdf>.

¹³ 47 C.F.R. Part 4; Federal Communications Commission, Network Outage Reporting System (NORS), <https://www.fcc.gov/network-outage-reporting-system-nors> (last updated July 5, 2018).

the economic wellbeing of our Nation.”¹⁴ USTelecom members also participate in collaborative public-private efforts to improve security and resilience.¹⁵ And, of course, their contracts with customers – particularly government and enterprise customers – typically include specific obligations relating to network security and resilience. In short, failure to ensure network security and resiliency subjects USTelecom members to commercial, regulatory, and reputational risk – risks that all telecommunications providers seek to minimize.

B. USTelecom Members Must Ensure Their Customers’ Privacy

In addition to their obligations to ensure network security and resiliency, USTelecom members must protect their customers’ privacy – not only because the law requires them to do so, but also because telecommunications providers know that customers

¹⁴ *New Part 4 of the Commission’s Rules Concerning Disruptions to Communications*, Report and Order and Further Notice of Proposed Rulemaking, 19 FCC Rcd 16830, 16833 ¶ 1 (2004) (adopting 47 C.F.R. Part 4).

¹⁵ 2013 NIPP Annex at iii (the Communications Sector-Specific Plan “represents a collaborative effort among the private sector; State, local, tribal, and territorial governments; nongovernmental organizations; and Federal departments and agencies to identify and work toward shared goals and priorities to reduce critical infrastructure risk”); Communications Security, Reliability, and Interoperability Council, *Charter of the FCC’s Communications Security, Reliability, and Interoperability Council*, Section 3 (Mar. 19, 2017), <https://www.fcc.gov/file/12251/download> (“The purpose of the Council is to provide recommendations to the FCC regarding ways the FCC can strive for security, reliability, and interoperability of communications systems.”).

place a premium on their ability to communicate free of unlawful third-party surveillance.

Setting aside legal mandates, consumers should be able to make a phone call or use the internet with confidence while maintaining their privacy. As such, USTelecom's members are committed to taking the steps necessary to ensure the privacy of their customers. Specifically, USTelecom members are focused on transparently disclosing to consumers their practices with respect to use and disclosure of user data, and honoring customer commitments concerning how their data will be collected and used. USTelecom members are similarly committed to maintaining network protections that minimize the risks of unauthorized access to and use of their customers' sensitive commercial and personal data.¹⁶

USTelecom members' data privacy practices remain subject to substantial federal and state oversight. With respect to "common carrier" voice telephone offerings, USTelecom members have long been subject to Section 222 of the Communications Act of 1934, as amended, 47 U.S.C. § 222, as well as its implementing regulations. 47 C.F.R. § 64.2001 *et seq.* Section 222 and the FCC's implementing rules require carriers to protect users' "customer proprietary network information," or "CPNI," governing the ways in which USTelecom members are permitted use that information, the nature of customer consent required for uses of CPNI, and the reporting requirements for data breaches involving CPNI. *Ibid.* Among other

¹⁶ See USTelecom, *USTelecom Issue Brief, Digital Privacy* (Apr. 2019), <https://www.ustelecom.org/wp-content/uploads/2019/04/USTelecom-Brief-Privacy-4.19.pdf>.

things, providers of common carrier telecommunications services must train employees in the appropriate treatment of customers' CPNI, 47 C.F.R. § 64.2009(b), (c), and "take reasonable measures to discover and protect against attempts to gain unauthorized access to" such information. *Id.* § 64.2010(a). These are just some of the privacy requirements applicable to telephone service, which the FCC has enforced vigorously.¹⁷ Separately, to the extent USTelecom members offer video services using "cable systems" or satellites, they are subject to distinct Communications Act privacy mandates, also enforced by the FCC. *See* 47 U.S.C. §§ 551, 338(i).

To the extent USTelecom members are providing offerings that are not common carrier telecommunications services – such as broadband internet access and video – their privacy practices are subject to oversight from the FTC. Section 5 of the Federal Trade Commission Act of 1914, as amended, 15 U.S.C. § 45, directs the FTC to take action to prevent "unfair or deceptive acts or practices in or affecting commerce." *Id.* § 45(a)(1). The FTC has invoked this authority in more than 100 enforcement actions related to privacy and security,¹⁸ often on the basis that defendants failed to fulfill commitments made in their privacy

¹⁷ *See, e.g., Verizon; Compliance with the Commission's Rules and Regulations Governing Customer Proprietary Network Information*, Adopting Order, 29 FCC Rcd 10303 (Enforcement Bureau 2014).

¹⁸ Federal Trade Commission, Privacy & Data Security Update: 2018, January 2018 - December 2018 (rel. Mar. 15, 2019), <https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2018/2018-privacy-data-security-report-508.pdf>.

policies or engaged in privacy practices that were unreasonable no matter how well disclosed they might have been.¹⁹ Finally, USTelecom members also are subject to myriad state laws governing their privacy practices.²⁰ Put simply, no matter what type of service a USTelecom member offers, it is subject to one or more legal frameworks requiring it to maintain user privacy. As explained below, USTelecom members' ability to fulfil these obligations will be seriously compromised absent the ability to control the software code carriers use to implement their network interfaces.

C. USTelecom Members Must Retain Flexibility to Innovate and Compete as New Business Models Arise

USTelecom's members must also retain their ability to compete in an increasingly contested telecommunications marketplace. Nearly 25 years ago, a bipartisan Congressional majority passed, and President Clinton signed, the Telecommunications Act of 1996. Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (1996) (1996 Act), codified as amended at 47 U.S.C. 151 *et seq.* This legislation was designed to introduce competition into a range of communications markets that had long been subject to state-enforced monopolies. As Congress declared in

¹⁹ A list of the FTC's recent privacy/data security cases is available on its website. See Federal Trade Commission, Privacy and Security Enforcement, <https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement> (last visited Feb. 18, 2020).

²⁰ See, e.g., California Consumer Privacy Act of 2018, ch. 55, 2018 Cal. Legis. Serv. 1807, codified at Cal. Civ. Code §§ 1798.100-1798.199.

the legislation’s preamble, the 1996 Act was meant “to promote competition and reduce regulation in order to secure lower prices and higher quality services for telecommunications consumers and encourage the rapid deployment of new telecommunications technologies.” 1996 Act, 110 Stat. at 56.

In the near-quarter-century since, the 1996 Act’s goal has been achieved. USTelecom members once served nearly every customer in their service areas with traditional landline networks. By the end of 2017 they served only about 12 percent of all business and residential subscribers, and data compiled by USTelecom indicate that that figure will fall to 7 percent this year.²¹ There are vastly more wireless subscriptions than traditional “landline” subscriptions in the United States today.²² Traditional cable companies serve virtually every geographic market in the United States, offering almost ubiquitous broadband service suitable not only for carrying residential video offerings, but also for simultaneously provisioning telephone service and satisfying the high-volume data and internet access traffic needs of residential and business customers.

This robust competition has inspired providers to offer better-and-better services at lower-and-lower prices. But this virtuous cycle – in which competition

²¹ USTelecom Industry Metrics at 5.

²² FEDERAL COMMUNICATIONS COMMISSION, VOICE TELEPHONE SERVICES: STATUS AS OF DECEMBER 31, 2017 2 (Aug. 2019) (“In December 2017, the data shows that there were 50 million end-user switched access lines in service, 67 million interconnected VoIP subscriptions, and 340 million mobile subscriptions in the United States, or 456 million retail voice telephone service connections in total.”).

begets innovation, which begets still more competition – can only progress if providers in fact retain the ability to innovate. Traditional telephone providers could not compete by offering dial-up internet access in a broadband era, nor could they win customers with promises of facsimiles in an age dominated by emailed PDF files. Fortunately, these companies *have* been able to compete, by moving beyond the technologies and offerings of the past and keeping pace with their competitors, whether those competitors send their traffic over cable networks, wireless radio access networks, or fiber-optic links. They must retain the ability to innovate – to reconfigure their networks, and to offer new services and capabilities, in order to meet customers’ fast-changing needs. As described above, network innovation is, if anything, *accelerating* as features and capabilities migrate from hardware to software. If USTelecom members and other providers cannot keep up – whether due to technological factors, a counter-productive intellectual property regime, or other factors – the competitive communications that has arisen in recent decades will suffer, harming consumers across the nation.

D. USTelecom Members Would Be Impeded in Achieving These Critical Goals if All Software Interface Were Ineligible for Copyright Protection

The position advanced by Petitioner here would eliminate copyright entirely as a tool available to network providers, impacting providers’ abilities to ensure security and resiliency, to protect customer privacy, and to maintain the ability to innovate and

compete. In particular, Petitioner contends that there can be no copyright in a “software interface,” which, again, it defines as “a means of connecting to, interacting with, or operating computer software.” Pet. Br. 5 n.2. This broad definition would rob telecommunications companies and their vendors of their ability to assert copyright’s protections over their implementation of software interfaces, harming consumers and the public interest.²³

In the era of SDNs, a finding that the code that implements software interfaces governing access to and the use of next-generation networks is not copyrightable would jeopardize the ability of USTelecom’s members to assert certain property rights in core network components. Such a ruling would effectively require telecommunications companies to hand the keys to their proverbial kingdoms to third parties without restriction – third parties whose own objectives could be inconsistent with, or even directly contrary to, those of the network operator’s. This development would be inimical to the needs of

²³ While USTelecom disputes Petitioner’s overly broad definition of “software interface,” it does not contend that every software interface is *per se* copyrightable, nor does it understand Respondent Oracle to suggest as much. Rather, USTelecom believes that a finding that a software interface (as defined by Petitioner) can *never* be copyrightable would be an extreme erasure of expressive and creative authorship as well as damaging to the telecommunications industry. As Microsoft rightly notes, the courts have recognized “[i]n the software context ... that copyright should provide protections for aspects of software *that reflect truly creative expression from piracy and other forms of identical copying.*” Br. of Microsoft Corp. as Amicus Curiae in Support of Petitioner at 4 (filed Jan. 13, 2020) (Microsoft Br.) (emphasis added).

communications consumers and to the public interest more broadly.

Legacy and evolving telecommunications networks necessarily utilize myriad software interfaces, many of which embody the creative expression required by copyright law and are thus protectable by copyright. Telecommunications companies, moreover, do rely on copyright to protect these innovative expressions. Copyright offers unique advantages, allowing a telecommunications provider to make their implementation of a software interface publicly available without sacrificing its property interest in the interface.²⁴ As in other industries, copyright enables participants in the telecommunications industry to “to license [their] own products and services and earn a fair return for [their] creations.” Microsoft Br. 2.

But the ability to distribute the code associated with a software interface without forfeiting associated property rights is *particularly* important in the telecommunications industry, because participants in telecommunications markets must interoperate and collaborate, even while fiercely competing. For more than a century, the telecommunications landscape has been governed by extensive interconnection arrangements, which allow customers of Provider A to speak or exchange data with the customers of Providers B, C, and D. Thus, whether a provider’s network relies on telephone wires, cable facilities, wireless

²⁴ See *Nat’l Comm’n on New Tech. Uses of Copyrighted Works*, Final Report, III.C.1.c (1979), <https://files.eric.ed.gov/fulltext/ED160122.pdf> (comparing copyright and other methods of protecting software) (CONTU Report).

spectrum, or another medium, the provider must implement interfaces on its network, and associated devices, to allow traffic to be sent to and from competing providers' networks. Interfaces – increasingly, *software* interfaces – are used to enable interoperability among technologies, networks, and devices. Thus, USTelecom members have no choice but to make their software interfaces available so that they and their competitors can exchange traffic and meet customers' needs.²⁵

Yet, while telecommunications providers must share access to their software interfaces, they also must retain their exclusive property rights in their implementation of these interfaces if they are to ensure network security and resiliency, protect their customers' privacy, innovate and compete. Even in previous generations of networks, USTelecom's members regulated access to their network and the data derived from their network through self-developed

²⁵ For similar reasons, modern telecommunications rely on a robust system of consensus, industry-adopted standards that enables interoperability and compatibility. Recognizing their value, the FCC has incorporated many of these standards into regulations as requirements and safe harbors. *See, e.g.*, 47 C.F.R. § 15.31(a)(4) (requiring the use of the ANSI C63.4-2014 testing standard to determine compliance with the FCC's technical requirements for unintentional radiators); *id.* § 79.103(c)(11) (deeming apparatus which implement Society of Motion Picture and Television Engineers Timed Text format (SMPTE ST 2052-1:2010) to comply with specific technical capabilities for Internet Protocol Closed Captioning). These standards are themselves copyrightable. Indeed, it is often the copyright in written materials that provides comfort to participants in a standard setting process that they can share such materials about their innovation and not have to take extra measures to protect the secrecy of their innovation.

software and software interface licenses. Those licenses provide them a level of control over what others can do – and learn from – their networks.

The ability to assert some ownership right in proprietary interfaces created for network access in an SDN world is critical to maintain security and privacy, and to invest without fear that their innovations will immediately be appropriated by others. Indeed, if all software interfaces were not copyrightable, a provider's incentive and ability to differentiate itself on the basis of innovative software interface design would collapse, because it would bear the entire cost of such innovation, whereas any *benefit* arising from its investment could easily be appropriated by its competitors. Copyright is an important tool in preventing all of these outcomes, and in enabling USTelecom's members to fulfill their various obligations.

E. Alternative Means of Protecting Property Rights in Software Interfaces Are Less Effective or Less Practical Than Copyright

As explained by the National Commission on New Technological Uses of Copyrighted Works (CONTU) Report²⁶ and as demonstrated by subsequent judicial decisions, other legal protections, including other forms of intellectual property right protections, are less well suited to fulfilling the dual imperative of making interfaces available and retaining control over those interfaces. For example, maintaining the code that a carrier uses to implement an

²⁶ See CONTU Report.

interface as a trade secret would defeat the interface's purpose as a connection to other products or individuals. SDNs must include interfaces that are specifically invoked by other products on a network or a human end user, and other programmers must be able to interact with the software implementing those interfaces. But the very act of making software available in that fashion could terminate its trade secret protection. This framework might be adequate for soft drinks, because drinking a Coke[®] does not require an understanding of its famously secret formula; shared use of a software interface, in contrast, often *does* necessitate such understanding.

Further, the process of attempting to obtain and enforce a software patent can be impractical and undesirable as compared to the relative ease of generating the “extremely low” level of creativity required of a copyrightable work. *Feist Publ'ns, Inc. v. Rural Tel. Serv. Co.*, 499 U.S. 340, 345 (1991). Copyright protection is automatic once the code is fixed in a tangible medium, 17 U.S.C. § 102(a), and obtaining a copyright registration is an inexpensive process.²⁷ In contrast, patent protection for software is available only when the inventor can prove to the Patent Office that the software concerns patentable subject matter and is non-obvious, among other requirements. 35 U.S.C. §§ 101, 103. The landmark software patent case *Alice Corp. Pty. Ltd. v. CLS Bank Int'l*, 573 U.S. 208 (2014), had a profound effect on both the registrability and enforceability of software and business method pa-

²⁷ United States Copyright Office, Copyright Office Fees, Circular 4 at 7-8 (Apr. 2018), <https://www.copyright.gov/circs/circ04.pdf>.

tents, dramatically narrowing the class of software eligible for patent.²⁸ Since *Alice*, the Patent Trial & Appeal Board, the Federal District Courts, and the Federal Circuit have invalidated hundreds of patents.²⁹ These developments have cast doubt on the suitability of patents as a means of protecting property interests in software.

Other protections, such as contract or tort, might also fail to provide sufficient protection to software interfaces. Whereas copyright affords nationwide protection, common-law frameworks require burdensome state-by-state processes, which likely would generate disparate rulings and prolonged uncertainty over any particular interface's status.

* * *

In sum, copyright protections provide an important tool to telecommunications providers such as USTelecom's members. These entities must satisfy a host of legal mandates and business imperatives. Doing so requires that they retain control over their network interfaces, which increasingly are software-based. Alternative means of protecting such control, such as patent, contract, and tort law, while offering potential remedies, do not provide the same remedies as copyright protection. As such, a ruling in favor of Petitioner's view that software interfaces and the

²⁸ See Kate Gaudry & Samuel Hayim, *Years After Alice: Eligibility-Rejections Outflow from a Different Part of the USPTO*, JDSupra (Mar. 5, 2019), <https://www.jdsupra.com/legal-news/years-after-alice-eligibility-70833/>.

²⁹ See Fenwick & Alice LLP, *Decoding Patent Eligibility Post-Alice Patent Eligibility Case Analysis Tool*, <https://www.fenwick.com/pages/post-alice.aspx> (last visited Feb. 18, 2020).

code that implements them may never be copyrighted would be inimical to the needs of communications providers and their customers – and thus incompatible with the public interest.

CONCLUSION

For the foregoing reasons, USTelecom urges the Court to consider carefully the potential harms to software-driven next-generation communications networks that would arise if all software interfaces were ineligible for copyright protection, even when they otherwise met the applicable criteria for such protection.

Respectfully submitted,

PATRICK R. HALLEY
*Senior Vice President,
 Policy & Advocacy*

USTELECOM – THE
 BROADBAND ASSOCIATION
 601 New Jersey Ave, NW
 Suite 600
 Washington, DC 20001
 (202) 326-7300
 phalley@ustelecom.org

February 19, 2020

RUSSELL P. HANSER
Counsel of Record

JENNIFER B. TATEL
 NICHOLAS G. ALEXANDER
 WILKINSON BARKER
 KNAUER, LLP
 1800 M Street, NW
 Suite 800N
 Washington, DC 20036
 (202) 783-4141
 rhanser@wbklaw.com

Counsel for *Amicus Curiae*