November 20, 2017

Ms. Marlene H. Dortch, Secretary

Federal Communications Commission

445 Twelfth Street, SW

Washington, DC 20054

*Via Electronic Filing*

|  |  |  |
| --- | --- | --- |
| In the Matter of  Restoring Internet Freedom | **)**  **)**  **)** | WC Docket No. 17-108 |

Dear Ms. Dortch,

I[[1]](#footnote-1) offer these ex parte comments to aid the Commission in reaching the proper conclusion in construing the nature of Internet Service, determining the regulatory classification of Internet Service (IS) over broadband networks, in creating the regulations that should apply to Internet Service providers (ISP), and in repealing the regulations that should not apply to such services. The comments consist of a blog post, an unpublished editorial, and an American Enterprise Institute research paper I’ve written on the subjects of:

1. Preempting state efforts to apply local regulations to ISPs with respect to net neutrality and privacy; and:
2. The benefits of applying uniform regulation to ISPs and other Internet platforms such as Twitter, Facebook, Google, Amazon, and the web tracking networks operated by such firms; and:
3. The FCC’s measurement program, Measuring Broadband America, reveals the fact that web-based platforms are falling behind broadband networks in terms of performance. This calls the “virtuous cycle” theory into question and suggests that platform inequality has more to do with performance than does ISP behavior. The rich platforms, such as the Big 5 (Apple, Amazon, Google, Facebook, and Microsoft) own their own CDNs but smaller sites do not.

It’s very important for the Restoring Internet Freedom order to make it clear that ISPs are protected by CDA 230 and that ISPs and other Internet platforms fall within federal jurisdiction.

Best regards,

Richard Bennett

## Appendix: 50 Shades of Needless Complexity: Avoiding Policy-Induced Outages

The Internet broke Monday morning. Not for everybody, of course: the outages just hit [people who get their Internet service from an ISP that uses Level 3 for backbone service](https://edgylabs.com/level-3-error-disconnected-major-u-s-states-from-the-internet/) and live in Mountain View, Denver, Portland, Chicago, Seattle, New York, San Francisco, Houston, Minneapolis, and Boston.

Unbeknownst to the ISPs, Level 3 (now owned by CenturyLink) was routing user transmissions into a black hole thanks to a “route leak”. Level 3 didn’t mean to do this, [but it happened for reasons we don’t precisely understand](https://www.theregister.co.uk/2017/11/06/level3_comcast_outage/).

Route leaks happen [dozens of times a year in various locations](https://www.wired.com/story/how-a-tiny-error-shut-off-the-internet-for-parts-of-the-us/). The most infamous example happened in 2008 when Pakistan tried to block YouTube. It leaked some bogus routes to YouTube and [all the world’s YouTube traffic converged on an ISP that couldn’t handle it](https://www.cnet.com/news/how-pakistan-knocked-youtube-offline-and-how-to-make-sure-it-never-happens-again/). Internet routing depends on something called BGP, and BGP isn’t very robust.

## Routing is Complicated

BGP (Border Gateway Protocol) was [created when the NSF backbone that used to connect the non-commercial Internet was decommissioned](https://tools.ietf.org/html/rfc1930) in the mid-’90s. At the time, the community needed a means to select from a number of backbone routing companies, and the backbones needed a means of providing service to customers but denying it to others.

BGP also needed to conform routing to national laws that forbade certain classes of data from traversing particular countries. While routing decisions are generally made on the basis of commercial agreements and efficiency, some data requires special treatment. One example is data with national security implications.

Other data needs to be routed in sub-optimal fashion because of [data localization rules and other national policies](http://www.computerweekly.com/news/450299188/Irish-data-protection-case-raises-US-national-security-issues). So BGP is more complicated than technical considerations warrant. As with all technical systems, the more complicated the Internet’s routing map gets, the harder it becomes to optimize it.

## Complicated Systems Tend to be Unreliable

Because routing is complicated, ISPs and other networks trust their partners to configure their BGP information correctly. It’s hard to check in any case, so there’s very little choice. If Level 3 says it can route from Denver to the Daily Beast in an optimal manner, Denver ISPs believe it unless and until this assumption is proved wrong.

This is what happened Monday. The best guess is that CenturyLink and its newly acquired subsidiary, Level 3, made a mistake while optimizing routes as a result of the merger.

Looking into the mess on Monday, I saw packets going from Comcast into a intermediary called scnet.net and failing to emerge to the desired destination. This probably happened because Level 3 broadcast route announcements that claimed scnet.net could take users to CDNs in Chicago that it couldn’t actually reach.

So clicking a link to some websites led to an endless wait for a page to load. This didn’t affect all sites, but enough to be troublesome.

## Let’s make routing more complicated!

Nobody prefers convoluted routing and BGP is complicated enough. Data localization policies are bad because they undermine the Internet’s reliability, efficiency, and economics. Internet services like to store data in a limited number of locations with good connectivity to ISPs and rely on internal controls to deal with national differences such as content restrictions, currencies, and tax rates.

It’s certainly possible for retailers to charge and pay local authorities the appropriate sales tax rates, but that’s also complicated. Sales tax for some goods has to take national, state, county, and city rates into account and once collected it has to be disbursed correctly.

For a very long time, Internet sales were exempt from sale tax in the US simply because it was too hard to handle. And now that it’s a fact of life, the burden of collecting it impacts small companies more than the large ones. Internet sales tax even created a [niche for services that handle the problem](https://www.avalara.com/small-business/avatax/?lsmr=Paid%20Digital&lso=Paid%20Digital&referrer=https%3A%2F%2Fwww.google.com%2F&lastReferrer=www.avalara.com&sessionId=1510110959191) for small retailers.

As far as I am aware, there is no corresponding service for routing. Assuring compliance with national laws is partly a backbone service but mainly a service provider headache.

## 50 Shades of Needless Complexity

US-based Internet companies that do business in Europe, Russia, and China had to adapt their services to local laws. While this is a nuisance, it’s not the major issue with localization: language and culture issues are also part of the bargain. And this kind of adaptation is not nearly as bad as it could be, because the 30 nations in Europe follow a uniform guideline.

Doing business across the US requires partnerships with backbones and a number of data centers. This is purely a technical arrangement that companies can easily adjust as their needs and scale change.

But what would happen if each of the 50 states and 16 territories had its own regulations on privacy, security, and net neutrality? We would effectively return to the scenarios that prevailed in Europe before the formation of the common market or the US before the Constitution was ratified.

That’s not exactly chaos, but it’s a lot of needless red tape, barriers to commerce, favors for local employers and meddling by public utility commissioners. Rather than the federalist utopia of 50 laboratories of democracy, we would simply have a less reliable national Internet.

This could easily impair the ability of US companies to compete on the global scale. The effort to accommodate 50 state laws would be greater than the effort to conduct business worldwide today. I wonder how many startups have the stomach for all of that.

## The Internet of Outages

Adapting services to state laws isn’t unheard of. Medicaid is a state level program administered by claims processors who’ve made a business out of portable accounting systems with policy modules easily adapted to specific state regulations.

If we apply Medicaid-style design to the Internet, we can envision policy modules responsive to state laws on:

* Tracking opt-ins
* Data retention
* Anonymization
* Data volume metering
* Site blocking criteria
* De-priotization of data under various conditions
* Routes between users and services
* Data compression for video streams
* Cookie permissions
* Warnings about data thresholds
* Switching between cellular and Wi-Fi and LAA under various scenarios
* Roaming onto other networks
* Myriad regulations on backhaul networks for small cells

That’s just off the top of my head, but it’s already about ten times more code than the entire Medicaid system. Whereas Medicaid is constrained by federal law with respect to the features it can customize, turning the states loose on Internet regulation without any limits would be a much more creative exercise.

As Internet services grow more complex, they become less reliable. While we can all appreciate the abstract benefits of a fair, free, and open Internet I suspect the average consumer is more interested in a reliable Facebook experience.

## Rational Federalism

In any field of interstate commerce, there will be some policy questions best suited to national consistency and others where variety is beneficial. The trick is to find the boundary between the two.

The wisdom of publicly-funded networks is hotly debated. So it makes sense for each state to enact its own framework about this question. The financing of a network doesn’t have any effect on its interconnection policies, so the Internet as a whole doesn’t care who’s footing the bill.

But opt-in vs. opt-out for Internet advertisers is a question with direct bearing on interstate commerce. And the question of applying opt-in to one segment of the Internet and opt-out to another raises additional legal and ethical considerations.

It would appear reasonable for the drafters of the FCC’s Restoring Internet Freedom order to examine key principles for instances in which experimentation at the state level is appropriate and helpful. The Commission is not all-knowing and all-seeing, so there’s nothing wrong with asking for help where it’s needed.

But I don’t expect there are going to be many places beyond fees, rates, and permissions where state level variation is going to be beneficial. Consistency is a virtue in its own right.

## Appendix: Change is the Internet’s Natural State

FCC Chairman Ajit Pai is expected to release the text of the [Restoring Internet Freedom order](https://www.fcc.gov/restoring-internet-freedom) on November 22nd. As we stand on the brink of resolving the net neutrality controversy yet again, [Congress is beginning to pay attention to the business practices of internet gatekeepers](https://www.nytimes.com/2017/10/31/us/politics/facebook-twitter-google-hearings-congress.html).

Some public figures are so enamored with net neutrality as to [imagine it a remedy for fake news rather than an enabler](https://www.wired.com/story/al-franken-just-gave-the-speech-big-tech-has-been-dreading/). The mere fact that such suggestions can be made, after 25 years of internet policy debate, shows that policy makers have fallen far behind our technology.

The internet has never been and can never be truly “neutral”. It’s a platform for many different users, devices, networks, and applications that neither impose the same burdens nor demand the same services. The internet is an historical oddity among communication technologies because it’s [the first designed to serve multiple needs](https://www.itif.org/files/2009-designed-for-change.pdf).

This flexible character nullifies the relevance of historical communication laws drafted with single-purpose networks in mind. Neutrality is [only verifiable when every user of a system is doing the same thing](http://hightechforum.org/neil-davies-part-2-ofcom-report/). And it’s not even the right name for the state of affairs its champions actually seek.

**Naturalistic Fictions**

The neutral internet has more in common with a grocery store chicken bearing an “all-natural” label than with a traditional network. The neutrality argument supposes that the internet has an essential nature that trumps policy because the internet’s “[code is law](https://harvardmagazine.com/2000/01/code-is-law-html)”.

But there’s nothing “natural” about chickens. The animal is a domesticated wild bird, the product of 8,000 years of directed breeding. Neither its feed nor its circumstances comes from Eden. Consumers play along with the fiction because natural goods provide us with [security blankets in a world of daunting technological wizardry](https://www.theatlantic.com/technology/archive/2015/10/americans-are-more-afraid-of-robots-than-death/410929/). Without thousands of years of human fiddling, the chicken doesn’t even exist.

The internet doesn’t have a natural state either. Its designers developed a computer-to-computer communications system within the constraints of the very limited technology extant in the [days of disco, the Nixon presidency, and the IBM and Bell monopolies](http://hightechforum.org/happy-birthday-internet-richard-bennett-talks-with-don-nielson/). The internet is defined more by its constraints than by its aspirations.

For the historical internet, the largest constraint of all was the lack of networking experience within the engineering community. When making design choices, the [pioneers couldn’t examine a body of literature for illumination](https://dl.acm.org/citation.cfm?id=1349793) because it didn’t exist. Hence, the guiding principle was: “[rough consensus and running code](https://groups.csail.mit.edu/ana/People/DDC/future_ietf_92.pdf)”, the programmer’s version of “it feels good, do it.”

**Taking Responsibility for Progress**

Making it up as we go along is fine as long as we’re learning from experience, as the internet has done on occasion. In the 1980s, we realized that the [only thing worse than one limited computer network was severa](http://www.internetnews.com/blog/skerner/30-years-of-tcpip-dominance-began-with-a-deadline.html)l. In the 1990s, we discovered that the internet would be more robust if it [lost the training wheels](https://www.nsf.gov/news/news_summ.jsp?cntn_id=103050) that connected universities to each other on the condition that no commercial activity took place.

In the 2000s, we learned [video streaming needed content delivery networks](https://qz.com/1001569/the-cdn-heavy-internet-in-rich-countries-will-be-unrecognizable-from-the-rest-of-the-worlds-in-five-years/), convenience stores that staged common goods close to users. And in the 2010s we came to understand that [mobility is more important than horsepower](https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html).

We now face the fact that some of things that have long been regarded as essential virtues – openness, the indiscriminate flow of information, anonymity, and a willingness to turn a blind eye to legal transgressions – are two-edged swords at best. The old media gatekeepers shaped the news to improve us, but [new media simply exploits our worst tendencies](http://hightechforum.org/great-social-media-freakout/).

**Universal Curation**

The fictions of mainstream media have been replaced by ideological bubbles where vicious falsehoods reign; Facebook in particular is awash with rabid enemies of vaccination, food fads, placebos, conspiracy theories, and false political narratives.

These bubbles exist because [current advertising models favor the intense engagement that’s most common among fanatics](https://www.axios.com/sean-parker-unloads-on-facebook-2508036343.html). Sowing distrust generates revenue. But it also creates disgust and depression in the long run, as studies of intense Facebook users have found.

There’s no better solution to social media maladies than quality control. Platforms serious about retaining users have to make their virtual neighborhoods more comfortable. Governing law such as [CDA 230 permits platforms to curate content, but doesn’t force them to shape it in any particular way](https://www.eff.org/issues/cda230). This is fine because those who fail at responsible curation are unlikely to succeed for long.

Making curation the norm rather than the exception also makes it easier for policy makers to impose specific mandates on platforms, such as the proposed ban on sex trafficking ads and long-overdue anti-piracy measures. But each such proposal is typically met with a combination of [crocodile tears, hand-wringing, and outright hysteria](https://www.wired.com/2012/01/websites-dark-in-revolt/).

These reactions are disingenuous. Platforms smart enough to target ads based on complex formulas and emotional insights can surely do a better job of identifying blatantly unlawful and reprehensible scams. The argument that social platforms are [too big to moderate](https://www.nytimes.com/2017/10/04/magazine/what-if-platforms-like-facebook-are-too-big-to-regulate.html) is ridiculous given the high revenues that come from large audiences for targeted ads. If we don’t have the technology to moderate at scale, we can create it.

**One Principle to Rule Them All**

The CDA 230 framework that’s been so good for content and communication platforms such as Google, Facebook, and Twitter also works for network platforms. In reality, there’s very little functional difference between a mobile LTE network and Twitter. Both platforms carry messages between [specified people without change in their content](https://www.law.cornell.edu/uscode/text/47/153), the traditional definition of a communications carrier. And both invest heavily in data centers, software, and network infrastructure.

Consumers do not expect either platform to behave indiscriminately. We want the ability to block cellular robocallers and to block Twitter trolls.  And we expect service providers to block service to criminal enterprises out to do us harm. We also expect them to handle voice and video as well as they manage text messages, even though rich content requires more resources.

Communication services work better, have broader appeal, and are more constructive when carefully managed. Fanciful ideas about a neutral and natural internet free of meddlesome technology stand in the way of our getting the internet we want.

Broadband networks provide more utility to more people when they are allowed to adapt services to application needs; we know this because it’s been proved in corporate and university networks.

**Help From Congress**

Consequently, broadband network regulation needs to move from the telecom model to a the CDA 230 platform model. Platform regulation needs to remain a largely light touch affair with carefully crafted exceptions.

When network platforms are governed by the same obligations that apply to social platforms, the prospects of sensible, verifiable, objective standards are maximized. Uniform regulation also brings an end to regulatory arbitrage between business sectors that are no longer genuinely distinct.

But this paradigm shift can’t succeed without an act of Congress. Fortunately, CDA 230 is under the microscope at the moment as lawmakers consider the Stop Enabling Sex Traffickers Act (SESTA), so any network-specific tweaks that may be needed can be made expeditiously.

Bringing Internet law up-to-date is always going to be a better bet than trying to shoehorn today’s technologies into yesterday’s models.

1. I am an independent network engineering consultant and policy analyst, presently working at High Tech Forum as editor and founder and as an independent consultant. These remarks are offered in my personal capacity and do not necessarily represent the opinions of any client or sponsor. I have previously offered comments in the “Protecting and Promoting the Open Internet” docket, GN 14-28, the “Preserving the Open Internet” and “Broadband Industry Practices” dockets, GN 09-191 and WC 07-52 respectively, and offered testimony at the [FCC En Banc Public Hearing on Broadband Network Management Practices in Cambridge on February 25, 2008](http://transition.fcc.gov/broadband_network_management/hearing-ma022508.html) as an invited technical expert. My CV is available at http://www.bennett.com/resume.pdf. [↑](#footnote-ref-1)