Before the

NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION

Washington, D.C. 20230

In the Matter of the	)	
	)	
International Internet Policy Priorities	)	Docket No. 180124068–8068–01
	)	
	)	

COMMENTS OF THE INTERNATIONAL CENTER FOR LAW & ECONOMICS

ICLE | 2117 NE Oregon St. Ste 501| Portland, OR 97232 | 503.770.0076
icle@laweconcenter.org @laweconcenter | www.laweconcenter.org

We would like to thank you for the opportunity to comment on these important and timely issues. In the preamble to this Notice of Inquiry ("NOI") the NTIA notes that is responsible for "protecting and promoting an open and interoperable internet, advocating for the free flow of information, and **strengthening the global marketplace for American digital products and services**."[1] We agree with the implicit assumption of this statement that it is possible to both promote an open Internet as well as protect the interests of American creators.

With this in mind, we would like to offer some comments on how best to assess the oft-asserted[2] tension between policies that purport to maximize freedom online and those that seek to protect the interests of rightsholders.

It is undeniable that, in some cases, the unfettered flow of information can contribute to the infringement of the intellectual property rights of American citizens and companies, and that this is contrary to NTIA's mission to promote the marketplace for American digital products and services. But it is also undeniable that the protection of intellectual property rights can promote both the creation of information and its dissemination. Our intellectual property laws reflect the congressional and judicial balancing of these dynamics: There is little reason to think that the legislative and legal principles that determine when content or its distribution is illegal offline apply any less when content is distributed online.

The flow of information is, in fact, never "unfettered." When considering the free flow of information online, the goal should be the same as it is offline: to increase the flow of *legitimate* information and to decrease the flow of *illegitimate* information.

Properly considered, there is no novel conflict between promoting the flow of information and protecting intellectual property rights online. While the specific mechanisms employed to mediate between these two principles may differ — and, indeed, while technological change can alter the distribution of costs and benefits in ways that must be accounted for — the fundamental principles that determine the dividing line between "legal" and "illegal" content and its distribution offline can and should be respected online.

---

[1] *International Internet Policy Priorities*, National Telecommunications and Information Administration (June 5, 2018) *available at* https://www.federalregister.gov/documents/2018/06/05/2018-12075/international-internet-policy-priorities#addresses (emphasis added).

[2] *See, e.g.*, Adam Satariano, *Tech Giants Win a Battle Over Copyright Rules in Europe*, N.Y. TIMES (July 5, 2018) *available at* https://www.nytimes.com/2018/07/05/business/eu-parliament-copyright.html ; Scott Shackford, *Europe Delays Plan to Destroy the Internet With Terrible Copyright Enforcement Proposal*, REASON (July 5, 2018) *available at* http://reason.com/blog/2018/07/05/europe-delays-plan-to-destroy-the-intern?utm_medium=email

The free flow of information

The basic distinction between legitimate and illegitimate information

Notwithstanding marginal debates about what constitutes "legitimate" information, it is broadly true that duly constituted, democratic states seek to deter both the unlawful distribution of content, as well as the distribution of unlawful content. In this regard there is little or no conflict between "advocating for the free flow of information" and "strengthening the global marketplace for American digital products and services." Both interests are served by respecting the underlying, "offline" legal status of information and its dissemination.

Of greater complexity is the balancing of the principles of comity afforded sovereign states — even non-democratic ones — under international law with the promotion of the free flow of legitimate information. One immediate and obvious concern is the extent to which authoritarian regimes can censor their citizens' expression. Political dissent is a critical feature of free societies; governance measures should seek to counter the diminution of expression rights under authoritarian regimes. The NTIA should thus pursue policies that aim to protect the expression of political dissidence (as well other milder forms of unpopular speech), consistent with broad principles of international law.

Yet while this tension may complicate some decisions regarding Internet governance, it does not substantially affect the fundamental alignment between the promotion of the free flow of information and the strengthening of the global, digital marketplace. For the vast majority of online information flows, the suppression of illegal content (or the illegal distribution of content) as determined by underlying, democratically constituted laws creates no novel conflict with the promotion of free expression. For the vast bulk of interactions online, the promotion of *legitimate* information may mean that some information is regulated — but this does not fundamentally impair the promotion of free expression where those regulations reflect legitimate social policy preferences.

Thus, for example, recent legislation designed to limit human trafficking and prostitution reflects Congress' determination that laws curtailing the exchange of information promoting these illegal activities should apply online, as well as off.[3] Whatever the merits or demerits of the specific implementation of this determination, it simply reflects the omnipresent tradeoff between the promotion of the flow of information and its regulation to implement other, legitimate policy preferences.[4]

---

[3] Allow States and Victims to Fight Online Sex Trafficking Act of 2017, H.R. 1865, 115th Cong. (2018) (enacted).

[4] Note, we do not take a position here on the advisability of FOSTA/SESTA in particular, but only use this to note that it is recognized by Congress that a fully unrestricted Internet is not desirable.

The extension of social and political preferences to the online world is necessarily fraught — but perhaps it shouldn't be. The Internet and other rapidly evolving technologies have dynamic effects on society. They can alter the assumptions upon which we have built our social institutions in ways that necessitate different legal and regulatory interventions than were previously necessary.[5] Our social and legal institutions should account for these dynamic effects.

Properly understanding freedom online

There is an important difference between "freedom" as a rule-less anarchy, and "freedom" as the ability of self-governed, moral agents to act within an open and equitable legal system. This latter, fuller sense of freedom is the foundation not only of government, but of civil society more generally. Technology, employed as tools that enhance and expand our ability to interact with the world, is an important component in the structures that lead to freedom:

> Technology is a key input into liberty, effectively defining what individuals can do: that is, defining the practical boundaries of an individual's liberty. And, as technological advance can expand the scope of these boundaries, it is often liberty-enhancing.[6]

However, technology may also constrain freedom. Hence, the, "effect [of technology] on liberty, autonomy, and the institutional environment may simultaneously push in opposing directions."[7] Thus, while technological advance should not be blithely deterred, nor should its sometimes problematic effects be ignored.

The Internet is emphatically not an ungovernable space, nor should it be regarded as such. To hold that there should be *no* restrictions at all on online data flows simply because they are facilitated by remarkable technological advance would lead to absurd results and diminish the thicker notion of freedom described above.

Indeed, even outside of intellectual property, the very structure of the Internet demonstrates the need for *some* form of regulation, whether privately-generated or otherwise. The Internet started as an explicitly non-commercial project to facilitate data sharing between government and academia. It wasn't until well after the core technologies were put in place that the Internet exploded to encompass universal access and widespread commercial activity. These

---

[5] *See, e.g.,* Justin (Gus) Hurwitz and Geoffrey A. Manne, *Classical Liberalism and the Problem of Technological Change* at 240 *in* THE CAMBRIDGE HANDBOOK OF CLASSICAL LIBERAL THOUGHT (M. Todd Henderson, ed. Cambridge Univ. Press 2018) (forthcoming) ("The effect of technological change on the institutional environment is particularly important and underappreciated. Changes that expand liberty for some people may also alter the relative incidence of transaction costs between contracting parties and thus alter or impair the (previously) efficient allocation of property rights. The institutional environment is not – nor should it be – static.")

[6] *Id.* at 238.

[7] *Id.*

core technologies were developed within a narrow community and for a narrow set of purposes. Thus constrained, the Internet embodied the idea that users could more or less be trusted, and those technologies therefore eschewed anything that would enable strong privacy, protections against cyber attacks, and, most relevant here, protection of legal rights to digital content transmitted across the network.

But these design limitations, although convenient for early Internet users, should not be mistaken as a justification for the perpetual repudiation of desirable legal constraints. Simply because privacy and security are made more difficult by the Internet's structure doesn't mean we should abandon the project of securing our networks going forward. Similarly, just because the Internet was built in a way that did not account for the legal rights of creators and inventors does not mean that those rights should no longer be protected online.

To allow the technological structure of the Internet to dictate its social and legal policies is needlessly fatalistic and manifestly undesirable. As the NOI notes, there are legitimate reasons for restricting the free flow of information, including "concerns about privacy, taxation and law enforcement access to data." Given the objective of "strengthening the global marketplace for American digital products and services" an additional justification for restricting the free flow of information is the protection of those digital products in order to enable creators and innovators to profit from their creation and distribution.

One might also note that, ironically, some of the same governments that impose the most egregious restrictions on freedom of expression also facilitate the rampant theft of American digital products and services. In other words, they restrict the free flow of information for nefarious reasons and fail to restrict it for legitimate ones. Thus, even on its own terms, a call for "pure" Internet freedom is anything but. **"Freedom" is always about making choices, and a preference for *no* rules is in fact a preference for a particular (and somewhat covert) system of control enabled by the Internet's technological characteristics.**

Encouraging more expression

It is a mistake, further, to regard expression rights and IP as in opposition to each other. Copyrighted works constitute an enormous amount of the content available online. When adequate systems are in place to enable the protection of IP, rightsholders are incentivized to create and share more content, thus increasing the extent and flow of information.

Moreover, there are real risks to Internet users because of the presence of illegitimate content. The most obvious harm that arises goes to one of the fundamental justifications for

trademark law: knowing the source and quality of a particular piece of content helps protect users from fraudulent distributors of inferior content.[8]

But fraud isn't the only concern. Consumers who access untrusted media files run the risk of infecting their machines with computer viruses.[9] Frequently, these attacks are undetectable to users until well after they have been infected, which makes it difficult for consumers themselves to be able to tell the "safe" illegal content from the "unsafe" illegal content. A widely available market for easily obtainable legitimate content goes a long way toward mitigating the spread of malware through illegal content.

Respecting jurisdictional boundaries

Technological change does not alter the moral aims of the law and neither does it necessarily undermine the scope of legitimate jurisdictional authority.

Leaving authoritarian concerns to the side for the moment, there is an acute interest among different countries in controlling the flow of illegitimate data that violates their domestic laws. Criminal rings use Internet services to traffic in illegal pharmaceuticals, as well as to commit property theft and a host of other crimes. After more than two decades of case law on the subject, questions relating to basic jurisdictional authority over Internet platforms remain evergreen.

To take one recent and contentious example, *Google v. Equustek* dealt with Canada's ability to require search engines to de-index links to infringing content on a worldwide basis.[10] Equustek, a manufacturer of networking equipment, obtained an injunction against former distributors who were making knock-off products. Equustek found its initial victory difficult to enforce, and commenced a familiar game of whack-a-mole, whereby the company would ask Google to take down a particular infringing Canadian URL only to have a new one spring up shortly afterward, both inside and, increasingly, outside of Canada. After a number of rounds of this game, Equustek asked Google to de-index all of the infringing URLs, both inside and outside of

---

[8] ICANN and WIPO forged an effective model for dealing with problems related to "passing off" in the domain name space. The Uniform Dispute Resolution Process — commonly known as UDRP — is a set of clear and simple rules that limit egregious abuse of the domain name system for the purpose of illegally exploiting trademarks. *See WIPO Guide to the Uniform Domain Name Dispute Resolution Policy*, World Intellectual Property Organization *available at* http://www.wipo.int/amc/en/domains/guide/

[9] Any file can theoretically be used as an attack vector in a computer through exploits that focus on common vulnerabilities, such as buffer overflow attacks. *See, e.g., Microsoft Windows Media Player ASX Playlist Buffer Overflow Vulnerability*, Cisco (Dec. 7, 2006) *available at* https://tools.cisco.com/security/center/viewAlert.x?alertId=12236

[10] Google Inc. v. Equustek Solutions Inc., 2017 SCC 34, [2017] 1 S.C.R. 824, ¶ 1 (Can.).

Canada, and Google refused. A Canadian appeals court subsequently sided with Equustek and required Google to de-index the infringing URLs.[11]

The Canadian Supreme Court ultimately sided with Equustek and issued an injunction that required Google to comply with the world wide de-indexing.[12] Subsequently, a district court in California preemptively sided with Google, and issued an order preventing enforcement of the Canadian order in the United States.[13]

A cornerstone of Google's position in the case was that intermediary liability must be circumscribed based on a court's geographic boundaries — otherwise, it argued, nations would be empowered to impose their own set of legal norms outside of their borders.[14] But this view is plainly at odds with the long history of courts parsing jurisdictional concerns, as well as determining liability based on often complicated and ambiguous factors. As the Canadian Appeals Court noted,

> [T]he threat of multi-jurisdictional control over Google's operations is, in my opinion, overstated. Courts must… consider many factors other than territorial competence and the existence of in personam jurisdiction over the parties… The extensive case law indicate[s]... that international courts do not see these sorts of orders as being unnecessarily intrusive….[15]

As noted above, "freedom" exists because of well-considered, public rules that facilitate civil society. And these rules are naturally capable of coming into conflict with each other, particularly when there are differences of opinion across jurisdictional boundaries. But the way to resolve these differences is not to ignore valid claims of jurisdiction — after all, Internet platforms certainly do operate in a way that affects the citizens of different jurisdictions. The way to handle these problems is to apply principles of comity that facilitate a reasonably satisfactory compliance with the laws of different countries.

The principle of comity largely originated in the work of the 17th Century Dutch legal scholar, Ulrich Huber.[16] Huber wrote that *comitas gentium* ("courtesy of nations") required the application of foreign law in certain cases:

---

[11] *Id*. at ¶ 20.

[12] *Id.* at ¶ 53.

[13] Google LLC v. Equustek Sols. Inc., No. 5:17-cv-04207-EJD, 2017 U.S. Dist. LEXIS 182194, at *8 (N.D. Cal. 2017).

[14] *Id.* at *4.

[15] Equustek Solutions Inc. v. Google Inc., 2015 BCCA 265, ¶ 56 (Can. B.C. C.A.) [hereinafter "Equustek Appeal Decision"].

[16] Joel R. Paul, *The Transformation of International Comity*, 71 L. CONTEMP. PROBS. 19 (2008) a*vailable at* https://scholarship.law.duke.edu/lcp/vol71/iss3/2

> [Sovereigns will] so act by way of comity that rights acquired within the limits of a government retain their force everywhere so far as they do not cause prejudice to the powers or rights of such government or of their subjects.[17]

And, notably, Huber wrote that:

> Although the laws of one nation can have no force directly with another, yet nothing could be more inconvenient to commerce and to international usage than that transactions valid by the law of one place should be rendered of no effect elsewhere on account of a difference in the law.[18]

The basic principle has been recognized and applied in international law for centuries. Of course, the flip side of the principle is that sovereign nations also get to decide for themselves whether to enforce foreign law within their jurisdictions. To summarize Huber (as well as Lord Mansfield, who brought the concept to England, and Justice Story, who brought it to the US):

> All three jurists were concerned with deeply polarizing public issues — nationalism, religious factionalism, and slavery. For each, comity empowered courts to decide whether to defer to foreign law out of respect for a foreign sovereign or whether domestic public policy should triumph over mere courtesy. For each, the court was the agent of the sovereign's own public law.[19]

Thus, in *Equustek*, because there were no sufficient, countervailing comity or freedom of expression concerns **in that case** that would counsel against such an order being granted, the interlocutory injunction was appropriate.[20]

Although the Internet presents some novel questions about the particular mechanisms of enforcement online, this novelty doesn't justify immunizing Internet firms from third-party court orders when they concern clearly illegal conduct that is within intermediaries' control, but difficult for courts to address directly. In fact, the law has long dealt with out-of-reach offenders by enjoining the conduct of intermediaries — for example, by prohibiting local stores from selling foreign-manufactured counterfeit goods, or requiring that taverns prevent patrons from driving drunk.[21] As Learned Hand wrote in 1930 in *Alemite Mfg. Corp. v. Staff*, a seminal case on this issue, although a court "cannot lawfully enjoin the world at large, no

---

[17] *Id.* at 22.

[18] Irina V. Getman-Pavlova, *The concept of "comity" in Ulrich Huber's conflict doctrine*, The National Research University "Higher School of Economics" at ¶ 13

[19] Joel R. Paul, *supra*, note 16 at 25.

[20] We are careful to note that there is not a presumption of widespread extraterritoriality, but that principles of comity do leave room for extraterritorial decisions, even on the Internet.

[21] Elizabeth Williams, *Validity, Construction, and Application of 18 U.S.C.A. § 2320, Criminalizing Trafficking in Counterfeit Goods or Services,* 90 A.L.R. Fed. 2d 113 (2018); *See also* Edward L. Raymond, *Social host's liability for injuries incurred by third parties as a result of intoxicated guest's negligence*, 62 A.L.R. 4th 16 (2018).

matter how broadly it words its decree… a person who knowingly assists a defendant in violating an injunction subjects himself to [injunctions by a court.]"[22]

The Internet may make this a bit more complex, but it's a difference of degree, not of kind. And, as the *Equustek* court observed, "it is the world-wide nature of Google's business and not any defect in the law" that makes it such that Google may have to assist courts in a variety of jurisdictions when faced with bad actors.[23]

The point here is not that the unique nature of Internet intermediaries should be ignored; it is of course important to understand that intermediaries' activities implicate a whole range of substantive issues that operate differently in different jurisdictions. Rather, the point is to stress that the proper approach is one that balances competing interests, not least of which are courts' abilities to effectively enforce their orders, even when that means issuing orders with extraterritorial effect.

Conclusion

Thank you again for the opportunity to comment on these timely and important topics. We believe that there is a way forward for Internet policy that both provides the freedom needed for users and Internet platforms as well as for rightsholders.

---

[22] 42 F.2d 832, 832-833 (2d Cir. 1930).

[23] Equustek Appeal Decision at ¶ 56.