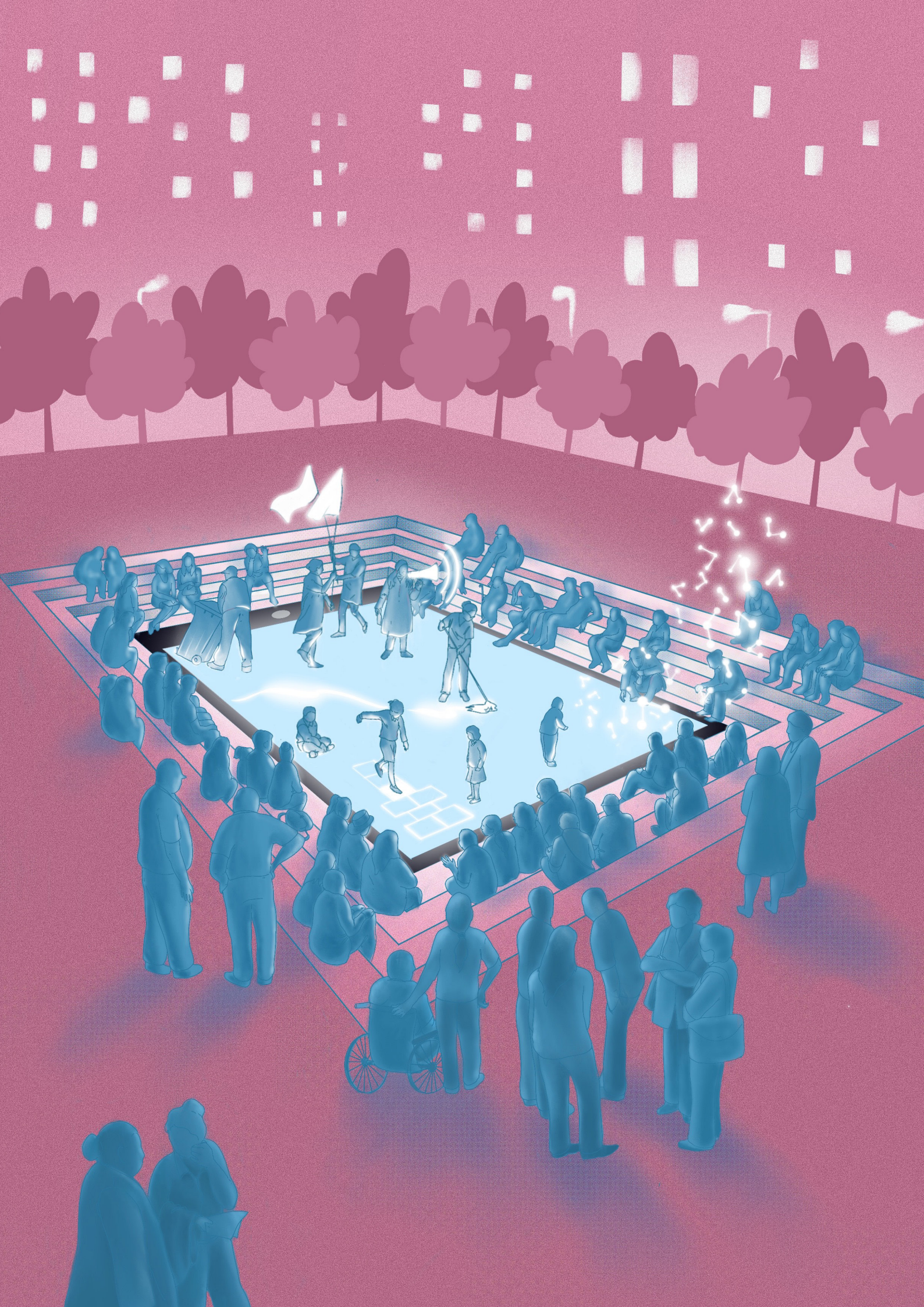

Roberto Bissio

...

The Coming Shift in Internet Governance

The internet could not exist without the common protocols and procedures for its constituent networks to link and transfer data between each other. How these protocols are decided upon is key to shaping a service that is currently used by nearly half of humanity. Yet, the 'governance of the internet' is not only about connecting devices, but also about what people are allowed, expected, or solicited to use these devices for. At the point when these protocols were first created, the internet was intended to be used solely for research and education, with any personal or commercial benefit being forbidden. This was the case until 1992, when previously fettered corporate greed became the driver of the 'internet boom'. Eventually, Section 230 of the Communications Decency Act, approved in 1996 by the US Congress, created the (rather weak) legal basis for social media and the gig economy by allowing on the internet activities which remained prohibited in the brick-and-mortar (and printed paper) world. The US ownership of the internet through ICANN and US-based monopolistic platforms is creating a 'governance bottleneck' precisely when the Covid-19 pandemic has made the internet an indispensable global public good. The time is ripe to usher in a new era for the internet.

Introduction

Back in 1989, in order to open my first dial-up account to access the internet at the vertiginous speed of 300 baud (bits per second, slower than the speed at which we read, but six times faster than telex!), I had to sign a written commitment to only use that powerful tool for research or educational purposes. I was to definitely not waste valuable bandwidth in "extensive use for private or personal business" and refrain from any "use for for-profit activities".

That was in Montevideo, Uruguay. The service provider was the public university but the conditions were imposed by National Science Foundation Network (NSFNET), the connectivity backbone of the National Science Foundation of the United States, which encompassed all connecting networks, irrespective of where they were located in the world.

As a journalist in a Latin American country just emerging from over a decade of military dictatorship, the lure of the internet, for me, lay in the possibility of accessing an enormous wealth of information and the promise of expanding freedoms. Yet, even when I was working for an NGO and profit was not my motivation for using the internet, it seemed odd that entry into this utopic 'cyberspace' required prior acceptance of a series of restrictions imposed by a foreign power.

1. A network for altruistic cooperation

The Internet Protocol and other data communication protocols identified by acronyms such as TCP, UDP, DNS, and BGP were initially developed in 1985 to connect the 'supercomputer centers' of five US universities funded by the National Science Foundation. NSFNET operated the 'backbone' — the actual cables allowing for high speed data communication from coast-to-coast between the five nodes — and then provided access, at no cost, to other universities and regional networks, and eventually, to any other network that was employing these protocols (although those residing abroad had to pay the whole cost of the international connection).

The TCP/IP protocol, initially developed on the Advanced Research Projects Agency Network (ARPANET) of the US Department of Defense, only determined **how** computer networks would be connected, but the 12 points of the Acceptable Use Policy (AUP) of NSFNET also clearly spelled out **what** users could or could not do. The AUP (of which I was required to sign a summarized Spanish translation) started by declaring that use of the network for any purpose other than "open research and education in and among US research and instructional institutions (...) is not acceptable". Communication with foreign peers for accepted purposes was legitimate "as long as any network that the foreign user employs for such communication provides reciprocal access to US researchers and educators" (Article 2).

Essentially, the internet started off being about researchers having remote access to supercomputers funded by taxpayers' money, through similarly subsidized data links. If a researcher or an educator were to derive any personal or commercial benefit from the use of these public resources, that would have been tantamount to a misuse of such resources, and become the subject of a scandal.

In reality, the AUP was not so much about policing individual usage, but determining which networks could or could not be connected to the backbone. A for-profit private institution could get connected for educational or research purposes, but a for-profit network charging for its services, or a network with businesses as clients, would not be eligible.

> The internet started off being about researchers having remote access to supercomputers funded by taxpayers' money.

The issue became more problematic when miniaturization brought computing out of big universities, state agencies, or corporations, and into individual homes and garage-based enterprises. In 1982, the home computer became *Time* magazine's "machine of the year". Empowered by these tools, users soon pressed to join 'the network'. The number of email addresses quadrupled between 1985 and 1989 to one million. By 1991, the number had further tripled to three million.

Many private networks sprang up to meet this demand, often developing their own protocols and new uses such as chatrooms and newsgroups. It was at this point that the AUP started being perceived as an obstacle. This was also a time when the US was celebrating its victory in the Cold War, an outcome frequently attributed to the country's technological advantages. A new Scientific and Advanced-Technology Act was voted in by the US Congress in 1992, based on the rationale that "the position of the United States in the world economy faces great challenges from highly trained foreign competition".[1] At the end of a series of measures to improve scientific and technological education, the Act included a cryptic amendment to the 1950 law regulating the National Science Foundation, now authorizing it "...to foster and support access by the research and education communities to computer networks which may be used substantially for purposes in addition to research and education in the sciences and engineering, if the additional uses will tend to increase the overall capabilities of the networks to support such research and education activities". The undefined "additional uses" of the internet would now be understood to include all kinds of for-profit traffic and activities.

2. Greed is good

That little amendment tore down the firewalls between commercial and non-commercial uses of the internet. The AUP continued to be the policy behind the NSFNET nodes, but the Network started to allow its backbone to channel traffic generated by commercial service providers without any control of its use. Thanks to this hidden subsidization of a new activity, the number of email addresses jumped to 25 million in 1996 and the Internet Protocol became the standard for computer-mediated communications, displacing alternative formulas such as the French Minitel, which attached a "dumb terminal" (screen and keyboard) to fixed telephone lines.

A sizeable proportion of the US population was already 'online' in 1996, when Congress approved another small amendment that would shape the evolution and

governance of the present-day internet and become the origin of many of its most persistent problems — from fake news to the informalization of work through the gig economy. In this amendment to the Communications Decency Act (CDA), a Section 230 was added, stating that, "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." The section boosted the internet by guaranteeing to digital publishers an immunity that does not exist in the material world.

Extreme messages are systematically given precedence over nuanced postings because the algorithms have 'learnt' that those messages get the most 'likes' or are reproduced faster and wider.

The consequences of Section 230 are evident in how the internet ecosystem has developed over the years. Social media, especially the most widely-used platforms like Facebook, Twitter, and the Google-owned YouTube have been exposed and criticized in recent years for channeling hate messages, propaganda, and disinformation, sometimes to the extent of influencing political processes in major countries and contributing directly to massacres, as in the well-documented case of the Rohingyas in Myanmar. The intentional and coordinated activity of 'trolls' (humans or automated message-generators called bots) exacerbates a trend already embedded in the algorithms that decide which messages are highlighted and made more visible. Extreme messages are systematically given precedence over nuanced postings because the algorithms have 'learnt' that those messages get the most 'likes' or are reproduced faster and wider. The obvious objective of such behavior is to maximize advertisement revenue, and the act of 'opening up the internet' to commercial activities usually gets a rap on the knuckle in this scenario. This, despite the fact that advertisements have been the main source of revenue for commercial radio and TV in many countries for decades, without generating similar problems.

What placed digital social media companies in a unique position, allowing them to evolve into platforms serving billions of users and simultaneously misusing the confidence vested in them by users, is the particular legal environment created by Section 230 and how it redefined publishing. The French Assembly established in 1789 stated that "the free communication of thought and opinion is one of the most precious[2] rights of man". But even in countries without actual censorship laws, the publisher of printed materials remains limited by provisions regarding copyright, questions of libel, obscenity, national security or "responsibility provisions". Freedom of speech does not allow one to cause panic by screaming "FIRE" in a crowded theatre and the publisher of a

recipe can be sued for damages if it results in poisoning. On the other hand, entities which are simply carriers of (someone else's) content cannot be blamed in any way for that content. For instance, the phone company is not responsible for obscene or threatening calls made through their lines.

When internet services started to be offered to the public, email could easily be likened to postal services: both were 'carriers', not responsible for the content of the messages they transmitted. But a publicly readable digital bulletin board made the digital service providing it liable as a 'publisher'.

In 1995, Prodigy Communications Corporation, an online service, which offered subscribers news, shopping games, and bulletin boards, was sued for libel after an anonymous user accused a banker of engaging in fraudulent acts. The Supreme Court of the State of New York ruled that Prodigy was "a publisher" — not simply a "carrier" — and therefore liable "because it had exercised editorial control by moderating some posts and establishing guidelines for impermissible content". If Prodigy had not engaged in any content moderation, it might have been granted free speech protections afforded to some distributors of content, like bookstores and news stands.[3,4]

Section 230 was meant to protect the perceived competitive advantage of the US in the digital realm by supporting emerging, and at the time rather experimental, platforms like Prodigy. It gave the digital publisher an immunity unavailable to those that published on paper. It also formed the legal basis for social media companies being able to generate enormous profits from content freely contributed on their platforms by the public they supposedly serve, without being liable for it.

Globally, in 1998, when the commercial uses of the internet were starting off, the World Trade Organization (WTO) decided to ban countries from applying customs duties on electronic transmissions. This e-commerce moratorium is still in effect, even after a research paper published by the United Nations Conference on Trade and Development (UNCTAD) in 2019 estimated that the potential tariff revenue loss to developing countries due to the moratorium was $10 billion in 2017.[5,6]

The e-commerce moratorium — India, South Africa, and other developing countries will push for it to be lifted during the coming WTO Ministerial Conference in 2021 — does not say anything about the content of electronic transmissions. But it does mean that countries find themselves practically unable to enforce their own publishing laws on social media companies operating from the US, and have to either accept the criteria laid down in Section 230 or ban these platforms altogether (and thus be seen as exercising censorship).

> **Section 230 is the legal basis of not just Facebook or Twitter, but all platforms that are part of the gig economy.**

Section 230 is the legal basis of not just Facebook or Twitter, but all platforms that are part of the gig economy. It allows ride-hailing and food delivery platforms like Uber, DoorDash, etc. to claim that they do

not actually hire the driver or the person delivering food to your home (which would make them responsible as employers), but only channel 'information' (the availability posted by the bicycle owner) to the pizza parlor looking to reach its customers. While a hotel chain is responsible for what it offers it guests, Airbnb is not liable for any claim made by hosts because it is a 'platform' for information providers who happen to have free rooms in their homes. Monopolies earning billions were thus created under an obscure appendix of a Decency Act, whose other articles were soon blocked by the courts for infringing on free speech.

In 2000, the European Union introduced an E-commerce Directive along similar lines as Section 230, limiting the liability of "information society services". However, courts have different interpretations of what that means. In 2017, the Court of Justice of the European Union granted to Airbnb the status (and benefits) of an "information society service" while in another ruling it decided to classify Uber as a "service in the field of transport", with different responsibilities.[7] However, the adoption by Europe of similar rules as US did not produce the desired effect of stimulating similar or competing European platforms. Facing the evidence of multiple problems caused by unfair competition and monopolistic practices, the Europeans started to discuss more stringent regulations and a comprehensive review was announced in 2020 as part of a new EU Digital Services Act package.[8]

3. The censored president

On October 6, 2020, two separate events coincided in inaugurating a new chapter in internet governance. First, the antitrust subcommittee of the US House of Representatives issued a 449-page report stating that "companies that once were scrappy, underdog startups that challenged the status quo have become the kinds of monopolies we last saw in the era of oil barons and railroad tycoons." The report concludes that "these firms have too much power, and that power must be reined in and subject to appropriate oversight and enforcement."

Directly targeting the four GAFA companies — Google, Amazon, Facebook, and Apple — the report makes a case for breaking up Big Tech, as was done in the past with Standard Oil or ATT when they gained monopoly power. There is no bipartisan agreement on the precise measures to be taken, with the Democrats pushing for a new law and some Republican members of the subcommittee preferring to rely on existing antitrust legislation, but the very recognition of this problem at the highest echelons of decision-making is a major step.

As this report was made public at the Hill, from the White House president Donald Trump tweeted a one liner: REPEAL SECTION 230!!!

A day prior, Twitter had blocked Trump's account after the president publicly posted the email address of a journalist, in violation of the platform's policy forbidding the sharing of private information without the consent of the affected person. Trump's preferred tool of communication with the public remained blocked until the offending tweet was removed.

The Democratic presidential candidate Joe Biden has also gone on record calling for the revocation of Section 230 on grounds

that “it [Facebook] is not merely an internet company. It is propagating falsehoods they know to be false”.

Implicitly, Trump wants these platforms to be neutral carriers and thus unable to censor him, while Biden seems to want a responsible publisher that checks the facts and is liable for known falsehoods. If Section 230 is repealed, an internet platform could be one or the other, but not both at the same time.

and employees, or of sellers and buyers of products and services will have to become more transparent and easier to regulate and be taxed by governments as anonymity is reduced or disappears altogether.

Workers, small businesses, responsible publishers, and governments will be the winners in this scenario. Huge platforms that are now widely recognized as damaging monopolies would suffer, yes.

What might Section 230, the "backbone of internet governance", be replaced with in the near future? The short answer and the best case scenario: nothing.

Irrespective of the outcome of the 2020 US presidential elections, it would not be far-fetched to expect that Section 230, the “backbone of internet governance” will change substantially in the near future. If that happens, what would it be replaced with? The short answer and the best case scenario: nothing.

Without Section 230 (and other equivalent legislations), the legal framework for publishing or carrying messages on the internet would be the same as in the offline world, meaning that publishers will have to be responsible for what they publish, and carriers will have no liability for, no say in, and no ownership over the content they carry. Online versions of trusted publications will be more valuable, and advertising will return from a few global platforms to local content producers. There will be some friction in short-term small value contracts negotiated through electronic means, meaning that the respective roles of workers

And they will most likely argue that such a change is an attack on liberties. But the limits on what can be said or advertised already exist, and offline regulations have also been implemented in the online world. For example, the FOSTA-SESTA[9] bills passed by US Congress in 2018 (promoted by Republican legislators but voted for, among other democrats, by Senator Kamala Harris) makes web platforms liable if they carry ads for prostitution, even though consensual sex work is not illegal in all US states. Following this legislation, sites that do not usually moderate content, such as Craigslist or Reddit, were forced to discontinue their personal ad sections in the US, even as they carried them in their websites for other countries. It is arguable if the FOSTA-SESTA acts actually reduce prostitution or only confine it to the ‘deep web’, but by making websites liable for content published by a third party, they do bore a hole in the flank of Section 230 and the (excessive) guarantees it provides to publishers.

With human rights caught between the corporate self-regulation practiced by the monopolistic platforms and the authoritarian regulation supported by many politicians to counter fake news, a group of Latin American researchers and civil society organizations have proposed a "third way". They call for an "asymmetric regulation" where the bigger the platforms are, the more responsibilities they should undertake.[10]

Ultimately, under human rights law, governments are the duty bearers and it is up to them to "respect, protect and fulfil" those rights, while the role of business is to "comply with all applicable laws and to respect human rights" an obligation that comes with "appropriate and effective remedies when breached".[11] No self-regulation can substitute the need for a legal norm, even when, these norms are established by the same governments which renege their human rights duties.

In the triangle formed by civil society, state, and the market, people hold rights, governments bear duties, and corporations are granted privileges. These privileges can only be justified if corporations meet expected outcomes and should be taken away when the collateral damage outweighs the expected benefits, or privileges are abused to build monopolies.

The Covid-19 pandemic made the internet an essential tool around the world, with the *Financial Times* arguing that "internet access is both a human right and a business opportunity".[12]

With a view to ensuring access to information as a right, in August 2020 the Argentinian government froze the tariffs of paid TV, internet, and fixed and mobile phone services, declaring them "essential and strategic competitive public services". While keeping these services in private hands, the government recovered its authority to regulate them closely.[13] On October 7, 2020, the House of Representatives in Colombia unanimously approved a bill declaring the internet an "essential public service" with the same legal status as the provision of drinking water, sanitation, or electricity. This recognition of universal access to the internet as a right should, over time, lead to government interventions to ensure accessible and competitive prices.

4. But... the internet (still) belongs to the US

Covid-19 has forced governments to ensure wider access to the internet in order to make "social distancing" possible. This push brings us closer to the aspiration of the internet as a "global public good". But the reality is that, in many ways, the internet is still owned by the US.

> The reality is that, in many ways, the internet is still owned by the US.

As mentioned earlier, the US government directly owned or funded the supercomputers linked by the Internet Protocol and the lines that carried the data. Gradually, those operations were transferred to the private sector. However, through the Department of Commerce, the US Government still controlled the assignation of a unique number (known as IP address) to every device connected to the internet and a unique name for some of them. Thus, the

internet user can type www.socialwatch.org and a Domain Name Server will drive the connection to http://52.117.222.8 which is the IP number of the computer hosting the desired webpage. The Internet Assigned Numbers Authority (IANA) hosts the root zone database that ensures the coherence of the system.

To understand the governance relevance of running IANA, think of the following example: In November 2019 the CEO of VPN.com, an internet corporation, wrote to President Trump[14] requesting, in addition to the existing sanctions against Iran, "to terminate all access to .ir domains by removing the .ir domain delegation from the DNS root zone until these sanctions are lifted." The same letter explains that "the primary impact of this action would eliminate all web access and e-mail service to .ir domains. This would cause massive economic and communication disruption to Iran across more than 1,131,300 .ir domains."

The good news, from an internet governance point of view, is that the US president does not have the power to impose such a decision any more, after former president Barack Obama transferred all of IANA functions from the US Commerce Department to the Internet Corporation for Assigned Names and Numbers (ICANN) in October 2016. The bad news is that the "multistakeholder governance" of ICANN — where corporations, governments, and end users have a say — is far from being genuinely multilateral, democratic, or fair. A non-profit organization incorporated under the laws of the State of California, ICANN is still a US institution, subject to the authority of US courts and federal executive agencies like the Office of Foreign Assets Control.

Following the Snowden revelations of 2013, and the increasing distrust of the US government by others such as China and Russia as well as its allies in the EU and Latin America, Obama in 2014 announced the intention to transition key internet domain name functions "to the global multistakeholder community". The US Congress, in a bipartisan resolution, added that it would not accept a proposal to replace the role of the US government on the internet "with a government-led or an inter-governmental organization solution".

The fact that the government of one country could unilaterally, and at whim, wipe out another from the internet is a huge obstacle in transforming the internet into a global public good.

Irrespective of the merit of the proposed sanctions, in international law, such measures against a country can only be imposed by the Security Council of the United Nations. The fact that the government of one country could unilaterally, and at whim, wipe out another from the internet and wreak havoc just by deleting a registry in a database is a huge obstacle in transforming the internet into a global public good.

ICANN was requested to produce a proposal

that could ensure "the security, stability, and resiliency of the internet DNS" (domain name system) and "maintain the openness of the internet". But, after two years of consultations, it was never defined what "openness of the internet" means.

Civil society proposed, and the human rights community celebrated as a victory, the new bylaws of ICANN which state that "respecting internationally recognized human rights as required by applicable law" is one of the "core values" of the organization. But a long caveat after that affirmation explains that "this Core Value does not create, and shall not be interpreted to create, any obligation on ICANN" and it "does not obligate ICANN to enforce its human rights obligations, or the human rights obligations of other parties, against other parties." A (forthcoming) legal analysis by the Harvard Business Law Review concludes that "the new aspirations in the Bylaws are drafted in a way that they carry little, if any, legal weight", and "amount to little more than a veneer intended to bolster ICANN's public image".[15]

On October 1, 2016, the US Department of Commerce officially stopped performing any internet-related functions and the responsibilities held until then by the National Telecommunications and Information Administration (NTIA), was passed on to ICANN. What was initially announced as a new model of global multistakeholder governance ended up being described in the official website of the NTIA as a "privatization of the DNS", since those functions previously performed by a public agency subject to congressional oversight are now in the hands of a private entity. As arbiter of the internet domain names, ICANN invoices 140 million dollars a year to the registrars that, in turn, rent the use of those names to the public. Most of the income pays for a staff of 400, earning on average $200,000 a year.

If there was hope for forging international confidence in the neutrality and fairness of ICANN back in 2016, that is much less likely now, after four years of the Trump administration during which the world has seen the US unilaterally abandon signed international commitments like the Paris Agreement on Climate, withdraw from the World Health Organization in the middle of the Covid-19 pandemic, and openly disdain treaty entities that the US itself pushed for, like NATO or the WTO.

5. A new internet era?

During the transition debates leading up to the establishment of ICANN, there was an alternative arrangement proposed in the form of an entity created by an international treaty and subject to the Vienna Convention on the Law of Treaties. This proposed international entity would have been founded by sovereign parties and would have had extraterritorial immunity even if it was headquartered in the US. US law does not apply within the perimeters of the UN headquarters in New York and Swiss law does not apply inside the building of the WTO in Geneva. Headquarters of international organizations have similar statuses as those of foreign embassies. The mechanisms of international law — immunity, and extraterritoriality — have evolved in this way precisely to make trade and diplomacy possible and to create entities outside of the jurisdiction of any single government.

Many stakeholders and advisors commented during the transition that, for the internet

to be free of undue government pressures and respect and promote human rights, ICANN should have extraterritorial status and immunity from government prosecution. This would have been possible only if it was an international organization created by a treaty.

Becoming such an entity doesn't mean that governments will run it. An international organization can have non-state actors as members and decision-makers. For example, the International Labour Organization is tripartite, with governments, workers, and employers of each member country sitting as equals in its assembly. The status of an international organization is also compatible with the condition imposed by the US Congress that ICANN not be "government-led". This is the case with the International Criminal Court (ICC), whose statutes protect the independence of its judges from any government interference. Yes, a treaty-making process can be cumbersome and take decades, but it can also be quite fast and efficient. The ICC was negotiated and ratified in less time than it took to rewrite the ICANN bylaws through a multistakeholder process.

representatives of communities affected by ICANN's policies, including the half of humanity that is not yet connected to any internet service. Currently, only those actors directly interacting with ICANN participate in consultations and while governments and civil society are represented, it is the big corporations that have the major say.

The alternative proposals were deemed "unrealistic" four years ago. Even passing on the reins of the internet from the US government to an NGO was criticized by a group of Republican legislators led by Texas Senator Ted Cruz as a "radical proposal". "Like Jimmy Carter gave away the Panama Canal, Obama is giving away the internet," Cruz said.[16] An official statement by (then presidential candidate) Donald Trump backed that view: "Congress needs to act, or internet freedom will be lost for good, since there will be no way to make it great again once it is lost."[17]

Once in the White House, Trump attacked other Obama-era legislations but not the new status of ICANN. No attempts were made to reverse the transition and, in 2018, the privatization was pushed further by an

> **A treaty defining the governance of the internet as a global public good could also define the composition of an external body to which it is to be accountable.**

Ideally, a treaty defining the governance of the internet as a global public good could also define the composition of an external body, completely independent of ICANN, to which it is to be accountable and whose composition can be deemed to represent the "global public interest". This can include

NTIA decision to stop controlling the prices set by ICANN "in line with the public policy priorities of the Trump administration".[18] As a result, ICANN negotiated a new agreement with Verisign, the firm that registers the .com domains, allowing it to gradually double its prices over the next 10 years.

The ICANN transition became a *fait accompli* and disappeared from US debates. But while other issues (like Section 230) seem more urgent, Trump's attempts to extend the US-China trade war into the realm of the internet, the Huawei boycott, or the TikTok ban in the US, do not bolster confidence in the future neutrality and impartiality of a US-based entity at the heart of internet governance.

The unsolved governance problems of the internet thus seem to converge and press for urgent changes. In less than 40 years, the nature of the internet shifted several times, metamorphosing from a cooperative endeavor among researchers and educators to a profit-led incubator of daring initiatives which later transformed into oppressive monopolies. These shifts were induced by political decisions about how to govern the internet and its usage. A new shift is due to start now. And this time, it cannot result from some arcane, opaque regulation. Instead, it must be the subject of an informed, transparent, and inclusive global debate and legitimate international decision-making.

From stakeholders to rightsholders

After a period of empasizing the role of stakeholders in international governance, a new momentum towards focusing more on *rightsholders* is apparent in the "Escazú Agreement" on "Access to Information, Public Participation and Justice in Environmental Matters", adopted on March 2018 and currently just one ratification short of entering into force.

The purpose of the Agreement, which is a legally binding treaty for its signatories in the Latin American and Caribbean region, is "to guarantee the full and effective implementation in Latin America and the Caribbean of the rights of access to environmental information, public participation in the environmental decision-making process and access to justice in environmental matters". In order to ensure those rights, "each Party shall encourage the use of new information and communications technologies, such as open data, in the different languages used in the country, as appropriate. In no circumstances shall the use of electronic media constrain or result in discrimination against the public."[19]

NOTES

1. Scientific and Advanced-Technology Act of 1992, Pub. L. No. 102-476, S.1146. (1992). https://www.congress.gov/bill/102nd-congress/senate-bill/1146
2. Merriam Webster. (n.d). Precious. In *merriam-webster.com*. https://www.merriam-webster.com/dictionary/precious
3. Legal shield for social media is targeted by Trump. (2020, May 28). *New York Times*. https://www.nytimes.com/2020/05/28/business/section-230-internet-speech.html
4. Morrison, S. (2020, May 28). *Section 230, the internet free speech law Trump wants to repeal, explained*. The Vox. https://www.vox.com/recode/2020/5/28/21273241/section-230-explained-trump-social-media-twitter-facebook
5. Banga, R. (2019). *Growing trade in electronic transmissions: Implications for the south*. UNCTAD Research Paper 29. https://unctad.org/system/files/official-document/ser-rp-2019d1_en.pdf
6. See Banga, Rashmi. (2020, July 16). *Should digitally delivered products be exempted from customs duties?* UNCTAD. https://unctad.org/news/should-digitally-delivered-products-be-exempted-customs-duties
7. *Reform of the EU liability regime for online intermediaries background on the forthcoming Digital Services Act*. (2020). European Parliament, Brussels. https://www.europarl.europa.eu/RegData/etudes/IDAN/2020/649404/EPRS_IDA(2020)649404_EN.pdf
8. See *The Digital Services Act package*. (n.d). europa.eu. https://ec.europa.eu/digital-single-market/en/digital-services-act-package
9. Fight Online Sex Trafficking Act, and stop enabling sex traffickers acts: Allow states and victims to fight Online Sex Trafficking Act of 2017, Pub. L. No. 115-164, H.R.1865. (2018). https://www.congress.gov/bill/115th-congress/house-bill/1865/text
10. See *Guidelines for the democratic regulation of the big platforms to guarantee freedom of expression online and a free and open internet*. (2020, August). observacom.org. https://www.observacom.org/wp-content/uploads/2020/08/Padr%C3%B5es-para-uma-regula%C3%A7%C3%A3o-democr%C3%A1tica-das-grandes-plataformas.pdf
11. *Guiding principles on business and human rights*. (2011). United Nations, New York and Geneva. https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf
12. Internet access is both a human right and a business opportunity. (2020, June 28). *Financial Times*. https://www.ft.com/content/872dc219-d4d8-4896-92d3-7f9d45a5ce90
13. Califano, B. (2020, August 24). *To guarantee connectivity in order to exercise rights*. Página 12. https://www.pagina12.com.ar/287301-garantizar-conectividad-para-el-ejercicio-de-derechos
14. See *VPN.com warns President Trump & ICANN to terminate all Iranian domain names*. Global News Wire. https://www.globenewswire.com/news-release/2019/11/26/1952376/0/en/VPN-com-Warns-President-Trump-ICANN-to-Terminate-All-Iranian-Domain-Names.html
15. Zalnieriute, M. (2020). Human rights rhetoric in global internet governance: New ICANN bylaw on human rights. *University of New South Wales Law Research Series, 2020 Harvard Business Law Review*, UNSWLRS. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3532991
16. Livingston, A. (2016, September 29). As Congress OKs spending plan, Cruz falls short in internet bid. *Texas Tribune*. https://www.texastribune.org/2016/09/29/congress-keeps-doors-open-cruz-falls-short-interne/
17. *Trump joins Cruz in attacking Obama's internet plan*. (2016, September 21). Politico. https://www.politico.com/story/2016/09/donald-trump-ted-cruz-obama-internet-plan-228489
18. Baldacchino, J. (2020, February 9). *Pourquoi une décision de Donald Trump va faire doubler le prix des domaines web en .com?* France Inter. https://www.franceinter.fr/societe/pourquoi-une-decision-de-donald-trump-va-faire-doubler-le-prix-des-domaines-web-en-com
19. Bárcena, A. (2018). *Regional agreement on access*

to information, public participation and justice in environmental matters in Latin America and the Caribbean. United Nations publication LC/PUB.2018/8/-https://repositorio.cepal.org/bitstream/handle/11362/43583/1/S1800428_en.pdf

ABOUT THE AUTHOR

Roberto Bissio is based in Uruguay where he coordinates the secretariat of Social Watch, an international network of citizen organizations that monitors sustainable development policies. He is co-editor of the Global Policy Watch and was a member of the advisory group to the CCWG Accountability Group of ICANN during the "transition".

ILLUSTRATION BY MANSI THAKKAR