Four Internets

Kieron O'Hara & Wendy Hall[*]

Accepted June 2019, forthcoming in Communications of the ACM

The vision of an open Internet is characteristic of Silicon Valley's tech pioneers. The free and efficient flow of packets of bits requires decentralisation to prevent bottlenecks occurring at the central points as the system scales, open standards to allow interoperability, and IP addresses to identify the right destination. We take this system for granted, but one doesn't need a very long memory to recall a time when IT was dominated by proprietary protocols like AppleTalk or DECnet, and when one couldn't easily send an email from AOL to Prodigy. Yet the Internet hasn't simply improved: it has evolved into an open system as a result of philosophical and political decisions, as well as technical ones [1, 2].

In these pages recently, Vinton Cerf argued that there is a fundamental division between the IP layer and the application layers of the Internet, which together function to keep the open Internet flowing, and what he called the "virtual political layer", higher in the stack where the content is consumed and judged. At the lower levels, protocols such as TCP, SMTP and HTTP ignore content, using only metadata such as payload types, timestamps and email formats. Cerf worries that constraints imposed on information at the upper levels will have effects further down the stack [3].

We concur with Cerf's assessment, but we must beware of concluding that values are only relevant to the upper levels where we worry about the social effects of processing information, while down below the Internet's plumbing just gets collections of bits to the right place in the right order as efficiently as possible [1]. Aiming for seamless interoperability, for example, is certainly important, but that should not be equated with being value neutral [4].

For those of a libertarian cast of mind, politics and engineering complement each other to create the **Silicon Valley Open Internet**. The free flow of information through the network supports and is supported by free speech and unrestricted association [5]. However, if liberty is unrestricted, individually rational behaviour may damage public goods. Efficient transfer of information is wonderful, unless the information is hate speech or a virus or sensitive personal data; it is already value-laden to suggest that we can meaningfully evaluate the efficiency of information flow independently of its content

Different nations and organisations regulate and constrain where they can. In our recent paper for the Centre for International Governance Innovation, *Four Internets*, we argue that some key geopolitical actors are projecting models of Internet governance, and consequently creating their own realities – alternative Internets to Silicon Valley's [6].

This does not mean that the Internet is (necessarily) fragmenting; we agree with Milton Mueller that 'fragment' is "the wrong word with which to approach this problem" [7]. However, we are not as

[*] Web and Internet Science Group, Electronics and Computer Science, University of Southampton, Highfield, Southampton, UK, SO17 1BJ, kmoh@soton.ac.uk.

sanguine as he that the network effects and economic benefits of a seamlessly connected Internet "will continue to defeat … systematic deterioration of the global technical compatibility that the public Internet created".

We also dissent from Mueller's narrow focus on sovereignty; the actors we describe push back against the logic of the Open Internet with ideologically-informed aspirations intended to provide models for the Internet as a whole, projecting ideals and foreign policy, not merely defending national sovereignty. Furthermore, on the multistakeholder governance model of the Internet, governments are not the only actors of importance [1]; others include engineers and hackers, civil society, lawyers, business, and private individuals with political agendas.

The different models we describe below all recognise the advantage of connection to the network. They can – indeed, do – co-exist in uneasy armistice, relying on those lower protocol levels to keep them connected, like a dysfunctional family sharing the family home. But they compete for influence to shape the Internet's development, often at the relatively high level of institutions and regulation, but also at the lower levels. As a specific example of how technical issues influence and are influenced by the higher-levels, the decision not to make IPv6 backward-compatible with IPv4 has opened up new avenues of development and freedom for innovation that have removed constraints to many alternative approaches to Internet governance.

What are these alternative Internets?

The birth of the Internet within the US military-industrial complex brought libertarians together in coalition with more hard-headed types. But this coalition is coming apart, and we are seeing a distinct vision emerge in tension with Silicon Valley's Open Internet, which we call the **DC Commercial Internet**. If we think of data and Internet resources as property, then on this view the walled gardens of the tech giants are legitimate creations of their owners, to exploit commercially as they think fit. Users find these gardens easy, useful and attractive. There is an oligopoly of giant companies, but, as Schumpeter argued, near-monopolies should be tolerated if they produce innovation – which the tech behemoths certainly have.

The distinction is most clearly seen in the interminable arguments over net neutrality [8]. The First Amendment prevents the government from abridging free speech – but does that mean that the government must therefore use its powers to promote free speech by preventing interference with the free flow of information by private actors? The Silicon Valley answer is 'yes', and net neutrality follows. The response of the Supreme Court (which has remained consistent for some decades, as Presidents have come and gone – hence our location of this ideology in DC), is 'no', and that, if a service provider wishes to censor the speech (i.e. slow down the packets) of its users, the government cannot prevent it without abridging the *provider's* free speech. On the DC Commercial Internet vision, net neutrality should be determined by the contract between provider and user.

Not everyone wants market solutions, however. A third vision imagines a more or less open Internet, on which good behaviour is the norm. Trolling, privacy invasion and fake news should be marginalised or regulated away by a strong civil society whose members are trustworthy and trusting. This vision is particularly popular in the EU, as a means of protecting "fundamental European values and principles" [9]. The well-ordered, self-regulating, responsible **Brussels Bourgeois Internet,** long an ideal, has been given teeth by the Court of Justice of the European

Union, in a series of aggressive interpretations of data protection and competition law. GDPR is perhaps its most powerful weapon, and some European data protection regulators are using it to project European values (and regulations) internationally, with some success – for instance, the Brazilian data protection law, the GDPL, is pretty similar,[1] while Tim Cook and Mark Zuckerberg have each canvassed the possibility of harmonising global laws around GDPR. Its influence reaches down the protocol stack – for instance, its championing encryption as best data protection practice will incentivise encryption in the application layer, where so many security breaches occur.

GDPR is not the only influence, though. A controversial new EU Directive on Copyright for the Digital Single Market[2] is expected to impact popular content sites such as YouTube or Twitter, while the UK has recently released a white paper intended to regulate harmful content on global tech platforms.[3]

Regulation is not the only response to openness and markets. A stronger view is that the Internet, the medium for so much human interaction, could be the means of creating social harmony, not disruption, by ensuring that it allows 'good' things to happen, and 'bad' things to be prevented. The Internet, in other words, can be used for social control, by authorities who define and judge 'social good'. This kind of paternalism comes in many tempting flavours, from the mild 'nudge' philosophy through to outright authoritarianism (active intolerance of dissent). It can be disastrous; a Ugandan tax on Internet connections, intended to discourage gossip, recently resulted in a massive fall in Internet subscriptions.[4] The leading light in this area is China, which has placed digital technologies at the heart of propaganda, public opinion and social control, and so we dub this fourth vision the **Beijing Paternal Internet**, although all governments find it attractive to some extent.

China's ambitions with respect to the Internet were made clear in a series of articles in this journal in 2018 [10]. Its own tech giants, Baidu, Alibaba and Tencent, have commercial freedom to develop innovative services, but work closely with government on a tacit national project both to create a cyber superpower and to manage data, search, commerce and other types of Internet access. A national data-driven 'social credit' system may well grow out of a series of pilots to use crowdsourced data to score the trustworthiness of citizens, penalise those who have failed to pay debts or fines, and reward those who make social contributions, such as by donating blood [11].

Other ideals exist, but they lack powerful geopolitical backing. One final model deserves a mention: the hacking ethic, the use of the Internet against itself, despite itself, to create a world in which truth is in the eye of the beholder and in which anyone's motives can be made to appear impure. This outlaw view has long been pursued by individuals (as President Trump memorably suggested, by "somebody sitting on their bed that weighs 400 pounds"), but it has been weaponised by some nations impatient of the international order and the rule of law, most notably Russia, whose President Vladimir Putin has long espoused the paranoid nihilism of the mystical nationalist

[1] https://gdpr.report/news/2018/08/21/brazils-general-data-protection-law-isnt-quite-gdpr/.
[2] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2018-0337+0+DOC+PDF+V0//EN.
[3] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf.
[4] https://www.theguardian.com/global-development/2019/feb/27/millions-of-ugandans-quit-internet-after-introduction-of-social-media-tax-free-speech.

philosopher Ivan Ilyin (1883-1954) [12].[5] This model, the **Moscow Spoiler**, is not a fifth vision for the Internet, because it doesn't push for a new Internet; it asks only an Internet upon which to be parasitic. It won't even trust that; Russia is reported to be preparing to test its cyberdefence capability by temporarily disconnecting itself entirely,[6] seeing security in separation [13].

We have associated these various models with geopolitical actors which proselytise them, or have given them their most distinctive twists. However, the actual policies of any government cannot be reduced to a single ideological viewpoint. To take one example, Russia's foreign policy uses the Internet aggressively, but it also wants to promote business and social stability, which require different ideas, while its policing of the opposition has spawned an impressive surveillance capability [14]. Conversely, many nations indulge in misinformation and hacking, not just the Russians – the CIA are hardly amateurs in the game. So the Moscow spoiler model is neither equivalent to Russian Internet policy, nor unique to Russia. We say only that some arms of the Russian government, together with nationalist actors in a shady private sector, have refined the spoiler model to the *ne plus ultra* of disinformation, and so they get the credit reflected in the name. The four positive visions can be combined creatively. For instance, Tim Berners-Lee's Solid project to re-decentralise the Web uses Silicon Valley openness as a means to "restore balance – by giving every one of us complete control over data, personal or not, in a revolutionary way", but the end is recognisably Brussels bourgeois, to stop the Web being "an engine of inequity and division".[7] Sadly, they more often vie with each other for supremacy. This matters. For instance, the future of AI will be to a large extent determined by the regulation of data. China may be well-placed in future to centralise data as its people are enthusiastic users of e-commerce and social media within an authoritarian context [15].

Furthermore, about 50% of the world has yet to be connected to the Internet. The potential for growth is in Africa, India, and China itself. Which visions make themselves attractive to countries coming online will influence how the Internet will develop over the next decade. India's electronic ID system Aadhaar, for instance, is an incredible effort to give usable identities to the currently unvoiced, but what an instrument of potential social control is also being created. At least 20 governments[8] are interested in an Aadhaar of their own, with the World Bank helping export it.

Each of the visions, unlike the Moscow spoiler model, has its merits. Openness is key to the efficient and effective flow of information. The DC vision has produced incredible innovation, genuinely valuable and free services, and networks of undreamt-of complexity and density. Meanwhile, both the Beijing and Brussels visions emphasise defending public goods against disruption.

It is not possible to force agreement between differing geopolitical forces and ideological positions. However, in a world where international relations are increasingly seen as a zero-sum game, we need to focus on the mutual advantages of Internet unity, even if it is divided into a series of *de facto* satrapies governed on different principles. This means we need to work out methods and principles for Internet governance that simultaneously accept the range of views about its role in

[5] https://www.nytimes.com/2014/03/04/opinion/brooks-putin-cant-stop.html?
[6] https://www.theguardian.com/world/2019/feb/12/great-firewall-fears-as-russia-plans-to-cut-itself-off-from-internet
[7] https://medium.com/@timberners_lee/one-small-step-for-the-web-87f92217d085.
[8] https://factordaily.com/aadhaar-india-stack-export/

society, preserve the open standards that have made it such a revolutionary and successful technology, and ensure that human dignity and privacy are respected. This is not a trivial task, and the future of the Internet may depend in particular on how data about individuals and groups is treated, and whether the current level of exploitation of data can be maintained without diminishing trust in the technology that provides it.

References

[1] DeNardis, L. *The Global War for Internet Governance*, New Haven: Yale University Press, 2014.

[4] Cerf, V.G. Ownership vs. stewardship, *Communications of the ACM*, 62, 3, 2019, 6, https://doi.org/10.1145/3310251.

[3] Cerf, V.G. The upper layers of the Internet, *Communications of the ACM*, 61, 11, 2018, 5, https://doi.org/10.1145/3281164.

[4] Shilton, K. Engaging values despite neutrality: challenges and approaches to values reflection during the design of Internet infrastructure, *Science, Technology, and Human Values*, 43, 2, 2018, 247-269, https://doi.org/10.1177%2F0162243917714869.

[5] Benkler, Y. *The Wealth of Networks: How Social Production Transforms Markets and Freedom*, New Haven: Yale University Press, 2006.

[6] O'Hara, K., Hall, W. *Four Internets: The Geopolitics of Internet Governance*, Centre for International Governance Innovation paper no.206, 2018, https://www.cigionline.org/publications/four-internets-geopolitics-digital-governance.

[7] Mueller, M. *Will the Internet Fragment?*, Cambridge: Polity Press.

[8] Nunziato, D.C. *Virtual Freedom: Net Neutrality and Free Speech in the Internet Age*, Stanford: Stanford University Press, 2009.

[9] EDPS Ethics Advisory Group .*Towards a Digital Ethics*, European Data Protection Supervisor, 2018, https://edps.europa.eu/sites/edp/files/publication/18-01-25_eag_report_en.pdf.

[10] Zaagman, E. China's computing ambitions, *Communications of the ACM*, 61, 11, 2018, 40-41, https://doi.org/10.1145/3239534.

[11] Creemers, R. Cyber China: upgrading propaganda, public opinion work and social management for the twenty-first century, *Journal of Contemporary China*, 26, 103, 85-100, https://doi.org/10.1080/10670564.2016.1206281.

[12] Snyder, T. *The Road to Unfreedom*, London: Bodley Head, 2018.

[13] Ristolainen, M. Should 'RuNet 2020' be taken seriously? Contradictory views about cyber security between Russia and the West, *Journal of Information Warfare*, 16, 4, 2017, 113-131.

[14] Soldatov, A., Borogan, I. *The Red Web: The Kremlin's War on the Internet*, New York: PublicAffairs, 2015.

[15] Lee, K.-F. *AI Superpowers: China, Silicon Valley and the New World Order*, New York: Houghton Mifflin Harcourt, 2018.