Preparing for a More Fractured Web

The central services under siege built global-scale networks. If policy trends hold, what comes next?

Andrea O'Sullivan

What's your worry about Silicon Valley? Most everyone has one. For some, it allows impolitic speech to flourish online. If you're like me, you're more bothered by the threat of targeted content controls. Or you might fear that some companies have just gotten a little too big. Maybe you dislike the entire ad-based business model supporting much of big tech. Maybe you're concerned about privacy. It could be a combination of many things. Whatever your persuasion, there is usually some good reason to resist big American technology companies.

This essay will not debate the merits or demerits of any particular tech criticism.

Readers can find many such commentaries tailored to their own liking elsewhere on the world wide web. Instead, I will discuss how the many forces converging against American technology companies may result in a new web that is less, well, *worldwide*. What might such an internet look like?

We already have a good inkling. Most people have heard of one longstanding internet faultline: the so-called Great Firewall of China.[1] Residents of China cannot easily access major parts of the global internet. Instead, popular non-Chinese apps and services are reproduced by Chinese companies for those within the Firewall. We have Google, they have Baidu. We have Facebook, they have Tencent. We have Twitter, they have Weibo. And so on. No wonder China's "netizens" and global web "surfers" rarely interact.

China is by no means alone. The OpenNet Initiative tracks internet balkanization through its Global Internet Filtering Map.[2] Countries such as Iran, Syria, Saudi Arabia, Turkey, and Russia have imposed filtering controls for various political, social, security, and infrastructure purposes. It is no coincidence that the worst offending nations are among the top agitators against the prevailing global order.

But traditional allies have started to turn as well. The EU's landmark General Data Protection Regulation (GDPR) made many US-based websites inaccessible to much of Europe[3]—users had to route around such geofencing with VPNs (Virtual Private Networks) or forgo access altogether. The EU-US Privacy Shield, which regulates interbloc data flows, is undergoing legal challenges in the European Court of Justice.[4] These trends herald a future where data localization, which limits how information can be used across borders, is the norm.[5]

Regulating data means regulating commerce. Although framed as a way to bring tech companies in line, data regulations affect anyone who engages in online commerce: that is to say, almost everyone with a computer and a connection. To a foreign retailer, for instance, data controls might as well be a trade control.[6]

Then there are content controls. Users have long been accustomed to copyright laws restricting certain media in different jurisdictions.[7] Now even user-submitted content is increasingly subject to stronger controls. Germany's NetzDG law to target "hate speech" requires platforms to appoint local censorship representatives to comply with government removal mandates within 24 hours.[8] A report from Justitia finds some 13 countries that have proposed or enacted laws modeled on this "digital Berlin Wall."[9]

Other countries target encryption. These strong digital security techniques help to conceal data. Yet they also frustrate law enforcement efforts to extract data. Measures like Australia's Assistance and Access Bill of 2018 require communications providers to build government backdoors into encryption technologies upon request.[10] In other words, anyone with a website accessible in Australia may be deputized as a government hacker. According to Global Partners Digital's World Map of Encryption Laws and Policies, some two dozen nations impose similar obligations on individuals.[11] Online security, too, is becoming even more uneven.

Even in the US, cracks are growing.

California's Consumer Privacy Act is styled in the vein of the GDPR; other states are considering similar legislation.[12] Proposals like the Lawful Access to Encrypted Data Act[13] and the EARN IT Act[14] take aim at encryption like Australia. The latter also threatens liability protections enjoyed by platforms through Section 230 of the Communications Decency Act.[15] If removed, platforms might more aggressively censor impolitic speech as has been done in Germany.

The net effect of these trends is to craft an internet experience that is far from universal. Should they continue, the default web will be more or less traditionally "open" depending on your location.

One reason the open web so quickly became "open" at all is that private companies and multi-stakeholder organizations provided the scale to support and connect global populations. Boosted by US policies such as Section 230 and the laissez faire *Framework for Global Electronic Commerce*,[16] American companies led the charge. No wonder they dominate today.

While this global scale undoubtedly increased access, it came at the cost of seeding centralized vulnerabilities. In other words, the same entities that were so instrumental in globalizing the social internet are also the ones that can be and are targeted to descale connectivity, whatever the justification.

Imagine an alternative history where America's technology policy combination of hands-off e-commerce regulation and liability protections for platforms did not exist. It is unlikely that the platforms that are so embattled today would have developed as they did. Lacking the scale and user accessibility that these companies provide, connectivity might still be limited to the technical few and to major institutions with the budgets and labor to navigate a fragmented computing and legal environment.

Or perhaps more development would have accrued to innovating *around* legal liabilities. If there is no central entity managing data, there is no central entity on which to place data transfer controls—governments would have to track down and control each individual user.

We are accustomed to the "walled garden" or trusted third party model of networking and computing today, but there are other options. For example, we do not rely on one platform to provide all email messaging. There are communications protocols—such as SMTP, IMAP, and POP3—that set out the rules that any entity can use to connect. Anyone can use a Gmail account or an encrypted email service or even set up their own server using the same rule set.

Much of the internet actually operates through protocols. The Department of Defense-developed TCP/IP sets the rules for how packets of data are sent. More people may be familiar with HTTP, which sets rules for how links are accessed online. Dozens of such protocols operate almost invisibly to form the internet protocol suite that supports the web. Although protocol rules are crafted by standards-setting bodies, their applications are decentralized.

Open source software projects provide other more decentralized alternatives. In contrast to proprietary software, where code is kept secret, open source projects are developed in public by anyone who wants to contribute. Because no one entity can conceal or control the software, open source projects offer more user freedom and perhaps more security (since bugs can be caught by the public). The downside is that open source projects can be non-user friendly or slow to add new features since they are often a hobbyist pursuit.

Large companies like Facebook and Google do not operate as protocols or open source projects. They are private and centralized. But there is no technical reason that this should be the case.

In some instances, protocol or open source alternatives already exist. For example, many people are unsatisfied by Twitter's content moderation policies. They can at any time host their own Mastodon instance and run an open source social network. Twitter itself has launched an initiative—called Blue Sky—to develop similar open and decentralized technical standards for social media.[17]

It is no coincidence that decentralized and open source projects have attracted new interest at the same time that data controversies and controls have proliferated. Cryptocurrencies like Bitcoin—which replace trusted third parties in financial transactions with a peer-to-peer network—are some of the most well-known.[18] Similar projects seek to route around trusted third party vulnerabilities in domains such as digital identity (decentralized identifiers or IDs),[19] server operations (Urbit),[20] and marketplaces (OpenBazaar).[21]

The biggest challenge with decentralized alternatives is that nobody uses them. Most internet users are locked into existing central platforms because of the "network effect."[22] A social network becomes more valuable as the number of connections increases. It is hard, but not impossible, to overcome network effects to compete with existing platforms. It is even more difficult to do this as an open source and perhaps unfunded project with no obvious route to monetization.

There is one other major difference—perhaps a downside—that such decentralized alternatives present. Centralized platforms compete by matching users with relevant content and other users. Decentralized networks are necessarily more opaque by design. Users are free to broadcast data, but these will be less "legible" to any intended or unintended audiences.[23] Where the platform-based web encouraged controllable virality, the protocol-based web encourages uncontrollable small-scale affinity grouping. This may be a good thing for people who wish to be discrete, but a challenge for those who seek attention.

The future of the internet may well be two-tiered. The besieged "open" web could limp along a little less openly than before. Barring significant cultural and policy change, jurisdictional data controls will continue to fracture the global internet experience. Particular platforms may come and go, but the central service provider model to which most internet users are accustomed would continue.

Then there could be a second web that is at the same time freer and more closed. This less legible web would consist of a protocol and open source software stack that is mostly federated or distributed. These tools could empower users to freely connect. Yet lacking a central matching service, the freeweb would mostly consist of cloistered private groups. More global messaging would be technically possible, but socially much more difficult.

The upshot for people with concerns about Silicon Valley is that they may soon have the tools to route around the third parties they dislike. The downside for people who enjoy the network effects that central platforms provide is that this kind of more global connectivity may be unavailable on both tiers of the new web environment.

Andrea O'Sullivan is the Director of the Center for Tech and Innovation Policy at The James Madison Institute

REFERENCES

1 Geremie R. Barme and Sang Ye, "The Great Firewall of China," *WIRED* (June 1, 1997) https://www.wired.com/1997/06/china-3/.

2 "Global Internet Filtering Map," OpenNet Initiative, accessed August 8, 2020, https://onimap.citizenlab.org/.

3 Jeff South, "More than 1,000 U.S. news sites are still unavailable in Europe, two months after GDPR took effect," *Nieman Lab* (August 7, 2018) https://www.niemanlab.org/2018/08/more-than-1000-u-s-news-sites-are-still-unavailable-in-europe-two-months-after-gdpr-took-effect/.

4 "The Court of Justice invalidates Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield," Court of Justice of the European Union, Press Release, No. 91/20 (July 16, 2020) https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf.

5 Vincent Manancourt, "Demise of Privacy Shield may be the end of U.S.-Europe data transfers," *Politico* (August 4, 2020) https://www.politico.com/news/2020/08/04/privacy-shield-data-transfers-391650.

6 Daniel Lyons, "GDPR: Privacy as Europe's tariff by other means?" *AEIdeas*, American Enterprise Institute (July 3, 2018) https://www.aei.org/technology-and-innovation/gdpr-privacy-as-europes-tariff-by-other-means/.

7 Jonathon W. Penney, "Privacy and Legal Automation: The DMCA as a Case Study," *Stanford Technology Law Review*, Vol. 22, No. 1: pgs. 412-486 (2019) https://law.stanford.edu/wp-content/uploads/2019/09/Penney_20190923_Clean.pdf.

8 "The Netzwerkdurchsetzungsgesetz (NetzDG) Network Enforcement Law," *Center for Democracy and Technology*, July 17, 2017, https://cdt.org/insights/overview-of-the-netzdg-network-enforcement-law/.

9 Jacob Mchangama, and Joelle Fiss, "The Digital Berlin Wall: How Germany (Accidentally) Created a Prototype for Global Online Censorship," *Justitia*, November 2019, http://justitia-int.org/wp-content/uploads/2019/11/Analyse_The-Digital-Berlin-Wall-How-Germany-Accidentally-Created-a-Prototype-for-Global-Online-Censorship.pdf.

10 Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018, No. 148 (2018) https://www.legislation.gov.au/Details/C2018A00148.

11 "World map of encryption laws and policies," *Global Partners Digital,* accessed August 8, 2020, https://www.gp-digital.org/world-map-of-encryption/.

12 Jennifer Huddleston and Ian Adams, "Potential Constitutional Conflicts in State and Local Data Privacy Regulations," *Regulatory Transparency Project of the Federalist Society*, December 2, 2019, https://regproject.org/paper/potential-constitutional-conflicts-in-state-and-local-data-privacy-regulations/.

13 S.4051 - Lawful Access to Encrypted Data Act, 116th Congress (2019-2020) https://www.congress.gov/bill/116th-congress/senate-bill/4051.

14 S.3398 - EARN IT Act of 2020, 116th Congress (2019-2020) https://www.congress.gov/bill/116th-congress/senate-bill/3398/text.

15 47 U.S. Code § 230 - Protection for private blocking and screening of offensive material, https://www.law.cornell.edu/uscode/text/47/230.

16 *The Framework for Global Electronic Commerce*, accessed August 8, 2020, https://clintonwhitehouse4.archives.gov/WH/New/Commerce/.

17 @jack, Bluesky Twitter announcement thread, December 11, 2019, https://twitter.com/jack/status/1204766078468911106.

18 Jerry Brito and Andrea O'Sullivan, "Bitcoin: A Primer for Policymakers," *Mercatus Center at George Mason University*, May 3, 2016, https://www.mercatus.org/publications/technology-and-innovation/bitcoin-primer-policymakers.

19 Drummond Reed et al., "Decentralized Identifiers (DIDs) v1.0: Core architecture, data model, and representations," *World Wide Web Consortium (W3C),* working draft, July 31, 2020, https://www.w3.org/TR/did-core/.

20 "Understanding Urbit," *Urbit*, accessed August 8, 2020, https://urbit.org/understanding-urbit/.

21 "The Story of OpenBazaar," *OpenBazaar*, accessed August 8, 2020, https://openbazaar.org/about/.

22 Michael Katz and Carl Shapiro, "Systems Competition and Network Effects," *Journal of Economic Perspectives*, Vol. 8, No. 2 (Spring 1994): pgs. 93-115, https://www.aeaweb.org/articles?id=10.1257/jep.8.2.93.

23 As laid out by James C. Scott in *Seeing Like a State*, "legibility" refers to a given social structure's ability to be measured and manipulated by some higher authority. A more legible arrangement is more susceptible to control than a less legible arrangement. See: Venkatesh Rai, "A Big Little Idea Called Legibility," *ribbonfarm*, July 26, 2010, https://www.ribbonfarm.com/2010/07/26/a-big-little-idea-called-legibility/.