Lecture

THE SPLINTERNET

MARK A. LEMLEY†

TABLE OF CONTENTS

I. Your Parents' Internet 1397
II. The Splintering of the Internet 1399
A. Nationalizing Software and Regulation 1400
B. Nationalizing Hardware Networks 1410
C. Nationalizing the Network Itself 1415
III. The Internet Is Worth Saving 1418
IV. What Can We Do? 1422
Conclusion 1426

I. YOUR PARENTS' INTERNET

John Perry Barlow, who was honored with a symposium here at Duke just last year, famously wrote, in 1996, what he called "A Declaration of the Independence of Cyberspace."[1] "Governments of the Industrial World," he wrote, "you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the

† William H. Neukom Professor, Stanford Law School; Partner, Durie Tangri LLP. Thanks to Anupam Chander, Rose Hagan, David Lange, Noah Phillips, Peter Swire, and the participants at the Lange Lecture at Duke, where this talk was given. This is a lightly edited version of a speech, and it reads like it. While I thought I had come up with a clever title, it turns out someone else beat me to it. *See* SCOTT MALCOMSON, SPLINTERNET: HOW GEOPOLITICS AND COMMERCE ARE FRAGMENTING THE WORLD WIDE WEB (2016). His focus, unlike mine, is on the history of the internet and its deep ties to government.

I gave this speech in January 2020, when only a few people had heard of COVID-19 as a distant problem. I have updated it but not revised it to take account of the changed world in which we are currently living. But I think the pandemic only makes the importance of the internet and global communication more important.

1. John Perry Barlow, *A Declaration of the Independence of Cyberspace*, ELEC. FRONTIER FOUND. (Feb. 8, 1996), https://www.eff.org/cyberspace-independence [https://perma.cc/WM35-AE92].

future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather."[2]

John Gilmore, another famous internet pioneer, in 1993 coined the famous aphorism "The Net interprets censorship as damage and routes around it."[3]

Now, that was a long time ago. You can tell it was a long time ago because we hadn't settled on what we were actually going to call the internet. Maybe it was cyberspace, maybe it was the net. Infobahn was floating around there at the time.[4]

These sentiments sound somewhat quaint by modern standards. But it's worth remembering—or learning—that the internet of that day was the underground pirate alternative to where everybody thought information technology was going. The corporate and government big boys had a plan: we were going to build broadband wires for an information superhighway. The information superhighway was going to deliver prepackaged content to you in a one-way pipe with five hundred channels of television.[5] And that was going to be our technology connection. The idea that we might actually want to share information ourselves rather than merely passively consume it hadn't made it into the consciousness of the people who were building the technology.[6]

The internet, by contrast—what supplanted the information superhighway—started as a niche government-academic project to

---

2. *Id.*

3. *See* Philip Elmer-Dewitt, *First Nation in Cyberspace*, TIME INT'L (Dec. 6, 1993), http://kirste.userpage.fu-berlin.de/outerspace/internet-article.html [https://perma.cc/AJ3J-JY8Y] (quoting John Gilmore).

4. *See Information Superhighway*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/information%20superhighway [https://perma.cc/KLX8-VRMT].

5. *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO/AIMD-95-23, INFORMATION SUPERHIGHWAY: AN OVERVIEW OF TECHNOLOGY CHALLENGES 16 (1995), https://www.gao.gov/assets/160/154844.pdf [https://perma.cc/92LZ-B8DN].

6. As an aside, this is the grain of truth to the oft-mocked claim by Al Gore that he invented the internet. He was instrumental in funding broadband connections to build the planned information superhighway. *See* David Mikkelson, *Did Al Gore Say 'I Invented the Internet'?*, SNOPES (May 5, 2005), https://www.snopes.com/fact-check/internet-of-lies [https://perma.cc/YN4L-83MZ] ("During my service in the United States Congress, I took the initiative in creating the Internet. I took the initiative in moving forward a whole range of initiatives that have proven to be important to our country's economic growth and environmental protection, improvements in our educational system." (quoting *Transcript: Vice President Gore on CNN's 'Late Edition,'* CNN (Mar. 9, 1999, 5:06 PM), https://www.cnn.com/ALLPOLITICS/stories/1999/03/09/president.2000/transcript.gore/index.html [https://perma.cc/A753-YLLE])).

allow academics and military folks to communicate together.[7] Indeed, in the early days of the internet commercial entities weren't even allowed on unless they had some connection to the Defense Advanced Research Projects Agency ("DARPA") and the research agencies.[8] It wasn't until 1991 that they actually had unrestricted access to what we think of today as the web.[9] What became the private internet started as a series of "walled gardens," a bunch of people who wanted to get together in small communities like the Whole Earth 'Lectronic Link—the "WELL"—or AOL, Prodigy, and CompuServe.[10]

What the internet did was something quite remarkable. It allowed people to connect outside those walled gardens. It allowed you to interact with someone who wasn't part of a preexisting community, who wasn't geographically near you, who wasn't in the same community of scholarship and the same community of thought with you. And that connection turned out to be extraordinarily and unexpectedly valuable.

II. THE SPLINTERING OF THE INTERNET

My thesis is that the internet is being balkanized. We are returning to walled gardens. Some of those walled gardens are run by private companies, but increasingly, they are being created by drawing national boundaries around the internet. I think this phenomenon is already far along, and there are powerful forces behind it. The balkanization of the internet is a bad thing, and we should stop it if we can.

Now, I'm going to pause here and note that there should be a fairly heavy presumption against my argument. I am not the first person to

7. Janet Abbate, *Government, Business, and the Making of the Internet*, 75 BUS. HIST. REV. 147, 147–49 (2001).

8. J. Postel & J. Reynolds, *Domain Requirements [RFC 920]*, IETF: IETF DOCUMENTS 2 (Oct. 1984), https://tools.ietf.org/html/rfc920 [https://perma.cc/M8VS-FWQB] (creating the top-level domains starting in 1985); John Naughton, *The Evolution of the Internet: From Military Experiment to General Purpose Technology*, 1 J. CYBER POL'Y 5, 5 (2016) ("For the first two decades of its existence, it was the preserve of a technological, academic, and research elite.").

9. Martin Bryant, *20 Years Ago Today, The World Wide Web Opened to the Public*, NEXT WEB (Aug. 6, 2011), https://thenextweb.com/insider/2011/08/06/20-years-ago-today-the-world-wide-web-opened-to-the-public [https://perma.cc/D6V6-2775].

10. *AOL's 'Walled Garden*,*'* WALL ST. J. EUR. (Sept. 4, 2000, 11:57 PM), https://www.wsj.com/articles/SB968104011203980910 [https://perma.cc/Z7V4-WB3F].

say that the internet is in trouble and is going to die.[11] And this is not even the first time I've said it.[12] The internet has shown surprising resilience, and we shouldn't just assume it's going to go away. Nonetheless, I hope to convince you that there is a real problem here and that we should be concerned about it.

A. Nationalizing Software and Regulation

One way to think about this problem is to take John Gilmore's aphorism and reverse it. John Gilmore said in 1993 that "[t]he Net interprets censorship as damage and routes around it."[13] The idea was that we had a distributed network that can avoid centralized control. Today, I think it's fairer to say that censorship interprets the internet as damage and routes around it. As I argue here, governments have, in fact, figured out ways to avoid or control efforts of the internet to get around their censorship.

So, let me start by trying to persuade you that we are balkanizing the internet. That might seem an odd claim. If you look around, by all accounts it's the giants of technology who increasingly run everything. Google, Facebook, and Apple are everywhere in our world. That seems like centralization, not decentralization.

That's true for most of you because you're in the United States. But outside the United States, things look very different. We worry in the United States about decades-dominant platforms, but those platforms aren't actually dominant in most of the world.

If you go to China, you will not find Google and Facebook at all, and you will not find Apple as a dominant player. The sites that dominate the Chinese internet ecosystem are WeChat, Baidu, and

---

11. *See, e.g.*, Sara Morrison, *The Trump Administration's Flawed Plan To Destroy the Internet as We Know It*, VOX (June 18, 2020, 3:40 PM), https://www.vox.com/recode/2020/6/18/21294331/section-230-bill-barr-josh-hawley-trump-internet-free-speech [https://perma.cc/5P63-BLRD] ("Section 230, the law that is often credited as the reason why the internet as we know it exists, could be facing its greatest threat yet."); Shelly Palmer, *The Death of the Internet? Stop Saying That*, AD AGE (Dec. 18, 2017), https://adage.com/article/digitalnext/death-internet/311673 [https://perma.cc/4SEX-BQX5] ("'If net neutrality is repealed, the internet will die!' I'm paraphrasing, of course, but this is what many proponents of net neutrality believe. My issue with this line of thinking is that the idea presupposes the internet was previously alive and well. It was not.").

12. *See generally* Mark A. Lemley, David S. Levine & David G. Post, *Don't Break the Internet*, 64 STAN. L. REV. ONLINE 34 (2011) (stressing that in 2011 two congressional bills posed serious threats to the internet).

13. *See supra* note 3 and accompanying text.

Tencent.[14] If you go to Russia, you'll find Yandex, not Google, as the dominant internet company.[15]

And I think, increasingly, this is going to turn out to be true in Europe, which is a bit of a special case. Europe is targeting and restricting U.S. companies on the internet for both policy and mercantilist reasons.[16] And I think they will end up either moving European consumers to separate European internet companies and internet technologies or, perhaps, co-opting U.S. companies in ways that still end up dividing the U.S. experience from the European experience.

If you look at the rest of the world, what you see is actually an ongoing nation-by-nation competition for who gets the internet. And that competition is not one that the United States is necessarily going to win. To date, countries like Brazil and India have been primarily adopting U.S. technology companies and U.S. technology platforms,[17] though there's reason to think that's about to change.[18]

But if you look at Vietnam, Thailand, Indonesia, Malaysia, and others, those countries are buying into the Chinese model.[19] And the

14. *China's Top 10 Internet Companies in 2019*, CHINA DAILY (Aug. 27, 2019, 6:40 AM), https://www.chinadaily.com.cn/a/201908/27/WS5d645fc1a310cf3e35567f97.html [https://perma.cc/R6RU-WHL4].

15. *With 56% of Market Share, Yandex Is Confirmed as the Leading Search Engine in Russia – Gargiullo: "The Key to Selling in Europe's Biggest Market,"* PR.COM (Oct. 10, 2019), https://www.pr.com/press-release/796700 [https://perma.cc/32XJ-L2B2].

16. Julia Reda, *Why Americans Should Worry About the New EU Copyright Rules*, MEDIUM: BERKMAN KLEIN CTR. COLLECTION (Dec. 20, 2019), https://link.medium.com/0BDd6WFMBab [https://perma.cc/557P-HRRE]. For further discussion of EU regulations, see *infra* notes 30–33 and accompanying text.

17. Matthew Capala, *Global Search Engine Market Share for 2018 in the Top 15 GDP Nations*, MEDIUM (Aug. 28, 2018), https://medium.com/@SearchDecoder/global-search-engine-market-share-for-2018-in-the-top-15-gdp-nations-2cf65c11e5f5 [https://perma.cc/B9DR-LB9R]; *World Map of Social Networks*, VINCOS BLOG (Jan. 2020), https://vincos.it/world-map-of-social-networks [https://perma.cc/LYT9-ZKU7].

18. *See infra* notes 37–46 and accompanying text.

19. Lulu Yilun Chen & Yoolim Lee, *The U.S. Is Losing a Major Front to China in the New Cold War*, BLOOMBERG (Apr. 15, 2019, 6:00 AM), https://www.bloomberg.com/news/articles/2019-04-14/china-wins-allies-for-web-vision-in-ideological-battle-with-u-s [https://perma.cc/3X86-3GW9] (noting that "Vietnam and Thailand are among the Southeast Asian nations warming to" China's restrictive internet governance model); Krishna N. Das, *Malaysia's 5G Plan a Potential Boon for China's Huawei*, REUTERS (Sept. 24, 2019, 3:20 AM), https://www.reuters.com/article/us-telecoms-5g-malaysia/malaysias-5g-plan-a-potential-boon-for-chinas-huawei-idUSKBN1W90RD [https://perma.cc/Z448-2NLT] (noting Malaysia's adoption of Chinese 5G technology); Ma Jingjing, *Chinese Tech Companies Flock to Indonesia To Capitalize on Booming Internet Economy*, GLOB. TIMES (China) (Dec. 23, 2018, 5:23 PM),

companies that end up running the internet in those countries will increasingly be the Baidus and WeChats of the world, not the Googles and Facebooks.

That's also true in many countries in Africa and even Latin America, where China is building the physical infrastructure,[20] and it's increasingly easy for them to also build the software and technological infrastructure. So, while many countries have dominant private internet players, they're not the same private player.

The competition is not just for what company runs large aspects of your life. Instead, I think it reflects competition between regulatory models that are going to determine whether the internet as we know it will continue to exist in any given country.

In the United States, we largely listened to Barlow, at least in the 1990s and at least where the sacred cow of intellectual property ("IP") wasn't at issue. We let the technology companies get largely free rein. They ended up controlling your data, and that's a potential problem for many people.[21] But by and large, people have been free to post what they want, and they've been free to share it on whatever platform they want. There's reason to think that's going to change in the current political climate. The U.S. internet is under a lot of pressure from a variety of sources.[22] But if it does change, it's as likely to be in the direction of less private filtering of content and more First Amendment protection for hate speech as the reverse.[23] So, I think the freedom of the U.S. internet, with its good and bad aspects, is and will remain the U.S. model.

---

https://www.globaltimes.cn/content/1133239.shtml [https://perma.cc/32VR-HLMX] (noting Chinese investment in tech in Indonesia).

20. Paul Nantulya, *Implications for Africa from China's One Belt One Road Strategy*, AFR. CTR. FOR STRATEGIC STUD. (Mar. 22, 2019), https://africacenter.org/spotlight/implications-for-africa-china-one-belt-one-road-strategy [https://perma.cc/YC9L-AXYV]; Pepe Zhang, *Belt and Road in Latin America: A Regional Game Changer?*, ATL. COUNCIL (Oct. 8, 2019), https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/belt-and-road-in-latin-america-a-regional-game-changer [https://perma.cc/76AL-34RT].

21. Sam Schechner, *Privacy Problems Mount for Tech Giants*, WALL ST. J. (Jan. 21, 2019, 6:30 AM), https://www.wsj.com/articles/privacy-problems-mount-for-tech-giants-11548070201 [https://perma.cc/8F4F-MXG8].

22. Both the left and the right have attacked § 230, the core law that preserves internet freedom from legal liability. Morrison, *supra* note 11. On the importance of § 230, see generally JEFF KOSEFF, THE TWENTY-SIX WORDS THAT CREATED THE INTERNET (2019), and Anupam Chander, *How Law Made Silicon Valley*, 63 EMORY L.J. 639 (2014).

23. *See* Mark A. Lemley, *The Contradictions of Platform Regulation* (Feb. 3, 2021) (unpublished manuscript) (on file with author).

IP is a big exception. U.S. copyright industries have tried for some time to shut down as much of the internet as possible.[24] I think they've given up trying to shut it down altogether, but they would like to lock it down to the extent possible.[25] One way they accomplish that is through geoblocking.[26] And increasingly, their efforts are being accommodated by U.S. tech companies who are coming to deals with the copyright companies to engage in various kinds of filtering.[27] But outside IP, the U.S. approach to the internet has been fairly laissez-faire.

In Europe, by contrast, the content industries and the government get more, and more effective, control over the internet than they do in the United States. IP is once again a big driver. The copyright industries in Europe are quite influential, and the political leverage that U.S. tech companies have had, at least until recently, in the United States is not present in Europe. There is also a kind of nationalistic bias

---

24. For discussion of this history, see, for example, Mark A. Lemley, *Is the Sky Falling on the Content Industries?*, 9 J. TELECOMM. & HIGH TECH. L. 125, 125–35 (2011), and Mark A. Lemley & R. Anthony Reese, *Reducing Digital Copyright Infringement Without Restricting Innovation*, 56 STAN. L. REV. 1345, 1349 (2004).

25. Copyright owners are now trying to replace the DMCA's notice-and-takedown regime with "notice and stay down," which requires internet intermediaries to find and filter out any content copyright owners consider infringing. *See, e.g.*, Jonathan Bailey, *Take Down and Stay Down—Rethinking the DMCA*, PLAGIARISM TODAY (Mar. 28, 2016), https://www.plagiarismtoday.com/2016/03/28/take-stay-rethinking-dmca [https://perma.cc/JPF9-YACC]. Europe recently adopted such a system. Council Directive 2019/790, art. 17, 2019 O.J (L 130) 92, 95 (EU). The U.S. Copyright Office recently issued a report suggesting that the DMCA be changed to impose more obligations on intermediaries. U.S. COPYRIGHT OFF., SECTION 512 OF TITLE 17 1–7 (May 2020), https://www.copyright.gov/policy/section512/section-512-full-report.pdf [https://perma.cc/WR6Q-3QXQ]. For criticism of these proposals, see, for example, Mark A. Lemley & Christopher Sprigman, Opinion, *Why Notice-and-Takedown Is a Bit of Copyright Law Worth Saving*, L.A. TIMES (June 21, 2016, 5:00 AM), http://www.latimes.com/opinion/op-ed/la-oe-sprigman-lemley-notice-and-takedown-dmca-20160621-snap-story.html [https://perma.cc/8VCH-9UYZ].

26. *See generally* Peter K. Yu, *A Hater's Guide to Geoblocking*, 25 B.U. J. SCI. & TECH. L. 503 (2019) (discussing "the copyright industries' increasing demands for the use of geoblocking").

27. Google, for instance, processes more than 2 million copyright takedown notices every day. Gina Hall, *How Many Copyright Takedown Notices Does Google Handle Each Day? About 2 Million*, SILICON VALLEY BUS. J. (Mar. 7, 2016, 7:28 AM), https://www.bizjournals.com/sanjose/news/2016/03/07/how-many-copyright-takedown-notices-does-google.html [https://perma.cc/9R5S-HQ3P]. And that is despite having spent hundreds of millions of dollars to build ContentID, a screening system for YouTube that proactively finds copyrighted content and blocks it or helps the copyright owner monetize it. YouTube has paid billions of dollars to rights owners through the system. James Hale, *YouTube Has Paid Out More Than $3 Billion to Copyright Holders Through Content ID*, TUBEFILTER (Nov. 7, 2018), https://www.tubefilter.com/2018/11/07/youtube-payouts-content-id [https://perma.cc/QL9A-LGAP] (reporting over $3 billion in payouts as of 2018).

or Eurocentric bias against U.S. tech companies.[28] And there's much greater concern with privacy in Europe than there has been historically in the United States, a concern that recently manifested itself in a European court order blocking transfers of data to the United States because of concerns about U.S. surveillance.[29] And all of that means the European Union is increasingly seeking, and increasingly getting, control over what goes out on the internet there.[30]

European governments use that control primarily, but not exclusively, for commercial or mercantilist ends. They want their newspapers to be paid more. They want control over copyrighted works. They want privacy, for both good and bad purposes.[31] Europe demands that companies not collect information about citizens, but it also wants its citizens to be able to hide bad public facts about them so that people can't find out bad things that they've done in the past.[32] Europe is also more likely than the United States to control various kinds of hate speech, whether it's Nazi memorabilia or other information that they find offensive.[33] But by and large, Europe doesn't look radically different than the United States. It's just that the various forces who want commercial or personal restrictions on the internet have more power there than they do here.

In China and Russia, the internet is effectively controlled by the political arm of the state, and those states are both surveilling and

---

28. James Kanter, *E.U., Accused of Bias Against U.S. Companies, Opens Tax Inquiry into French Utility*, N.Y. TIMES (Sept. 19, 2016), https://www.nytimes.com/2016/09/20/business/international/europe-us-tax-luxembourg-engie-vestager.html [https://perma.cc/UVD4-XTNJ]; Richard Waters & Sam Fleming, *Google's Friends and Foes Draw Line Over 'Anti-American Bias*,*'* FIN. TIMES (June 26, 2017), https://www.ft.com/content/f16372d2-5aea-11e7-9bc8-8055f264aa8b [https://perma.cc/5LGT-X9ZZ].

29. A preliminary order has been issued. Sam Schechner & Emily Glazer, *Ireland To Order Facebook To Stop Sending User Data to U.S.*, WALL ST. J. (Sept. 9, 2020, 1:19 PM), https://www.wsj.com/articles/ireland-to-order-facebook-to-stop-sending-user-data-to-u-s-11599671980 [https://perma.cc/3QN8-FZKM]. The order is implementing a recent decision holding that where data is transferred to third countries, those countries must comply with EU standards. Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd., Maximillian Schrems, ECLI:EU:C:2020:559, ¶ 203 (July 16, 2020).

30. ANU BRADFORD, THE BRUSSELS EFFECT: HOW THE EU RULES THE WORLD xii–xix (2020).

31. *Id*. at xiv, 248–49.

32. For a discussion of the European "right to be forgotten" and its abuse, see Daphne Keller, *The Right Tools: Europe's Intermediary Liability Laws and the EU 2016 General Data Protection Regulation*, 33 BERKELEY TECH. L.J. 287, 287 (2018).

33. *See, e.g.*, Adam Satariano, *Britain Empowers Watchdog to Push for Policing of Internet Content*, N.Y. TIMES (London), Feb. 13, 2020, at B4.

locking down speech they don't like. You can't talk about democracy, Falun Gong, Tiananmen Square, or more recently, Hong Kong elections on WeChat[34] or you'll just get shut down. That works because China has built a censorship system that works with the Chinese apps and software that almost everyone uses in those countries.[35] And it has blocked or driven out many of the software programs that might challenge that censorship system.[36]

India is an interesting example of a country that has traditionally had a relatively open internet but which seems to be moving very heavily in the direction of locking it down. They shut down the internet altogether in Kashmir for several months as part of a political attack and crackdown on the Muslim population there.[37] And that model, I think, is increasingly likely to be used in India.

It's also increasingly likely to be used by authoritarian regimes around the world or authoritarian wannabes. These countries learned from Arab Spring the power of technology to potentially foment a revolution.[38] And if you're an authoritarian government, you don't want a revolution. So, they want to be able to control—to lock down—the means of communication.[39] And they've learned from various other examples, such as China, Russia, and India, that they can shut down either individual companies—blocking Facebook until they take down posts they don't like, for instance, or blocking Google until they do various things—or even that they can block the internet altogether to

34. Zoe Schiffer, *WeChat Keeps Banning Chinese Americans for Talking About Hong Kong*, VERGE (Nov. 25, 2019, 1:02 PM), https://www.theverge.com/2019/11/25/20976964/chinese-americans-censorship-wechat-hong-kong-elections-tiktok [https://perma.cc/32EG-UYJ8].

35. Elizabeth C. Economy, *The Great Firewall of China: Xi Jinping's Internet Shutdown*, GUARDIAN (June 29, 2018, 1:00 PM), https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown [https://perma.cc/LN75-NELM].

36. Julie E. Cohen, *Networks, Standards, and Network-and-Standard-Based Governance*, *in* AFTER THE DIGITAL TORNADO 58, 72 (Kevin Werbach ed., 2020); Jennifer Daskal & Paul Ohm, *Debate: We Need To Protect Strong National Borders on the Internet*, 17 COLO. TECH. L. REV. 13, 19 (2018) ("China, Russia, Bahrain, and Saudi Arabia, for many years, have engineered central points of control and failure into communications networks.").

37. Aijaz Hussain & Sheikh Saaliq, *Security Lockdown Severely Curtails Internet Access*, S.F. CHRON., Feb. 15, 2020, at A5; Jeffrey Gettleman, Vindu Goel & Maria Abi-Habib, *With Protests on the Rise, India Makes a Habit of Blocking the Internet*, N.Y. TIMES (New Delhi), Dec. 18, 2019, at A5.

38. Marc Lynch, *How Arab Authoritarian Regimes Learned To Defeat Popular Protests*, WASH. POST (Aug. 25, 2016, 5:00 AM), https://www.washingtonpost.com/news/monkey-cage/wp/2016/08/25/how-arab-authoritarian-regimes-learned-to-defeat-popular-protests [https://perma.cc/TN9S-QBK4].

39. Daskal & Ohm, *supra* note 36, at 19.

prevent dissidents from organizing. Iran,[40] Turkey,[41] Malaysia,[42] Brazil,[43] Pakistan,[44] and various Arab countries have all blocked large parts of the internet at one time or another.[45] Brazil has been most explicit. It has announced its intention to create a national, walled-off internet on the China model.[46]

It's not just differences in local regulations that are leading to different software in different countries. Rather, it's increasingly hard for foreign internet programs to penetrate local markets as a structural matter. Russia, for instance, has blocked LinkedIn,[47] is requiring local Russian apps to be loaded on all smartphones,[48] and is indeed writing its own version of Wikipedia.[49] Russia doesn't like the fact that on

40. Melissa Etehad & Ramin Mostaghim, *When Iran Blocked the Internet, Tech Experts in the U.S. Tried To Hack a Solution. Here's Why They Couldn't*, L.A. TIMES (Dec. 17, 2019, 3:00 AM), https://www.latimes.com/world-nation/story/2019-12-17/iran-blocked-internet-tech-experts-hack-solution [https://perma.cc/TG8A-KGCT].

41. Taylan Bilgic, *Turkey's Wikipedia Ban Violates Rights, Top Court Says*, BLOOMBERG (Dec. 26, 2019, 4:43 AM), https://www.bloomberg.com/news/articles/2019-12-26/turkey-s-wikipedia-ban-violates-rights-top-court-says-anadolu [https://perma.cc/9ZAL-BQPG] (discussing Turkey's ban on Wikipedia because the Turkish government didn't like how its policies were described there, and noting previous Turkish bans on Twitter, YouTube, and Facebook for political reasons).

42. Jeremy Malcolm, *Malaysian Internet Censorship Is Going from Bad to Worse*, ELEC. FRONTIER FOUND. (Mar. 7, 2016), https://www.eff.org/deeplinks/2016/03/malaysian-internet-censorship-going-bad-worse [https://perma.cc/32G2-TPFR].

43. *Judge Orders Block of Facebook Throughout Brazil Over Parody Account*, ACCESS NOW (Oct. 10, 2016, 6:01 PM), https://www.accessnow.org/judge-orders-block-facebook-throughout-brazil-parody-account [https://perma.cc/9T6E-S6WK].

44. Vindu Goel & Salman Masood, *Tech Giants Rebel Against Pakistan's Censorship Rules*, N.Y. TIMES (Mumbai), Feb. 28, 2020, at B1.

45. For a discussion of internet shutdowns worldwide, see generally Giovanni de Gregorio & Nicola Stremlau, *Internet Shutdowns and the Limits of Law*, 14 INT'L J. COMM'N. 1 (2020).

46. Nancy Scola, *Brazil Begins Laying Its Own Internet Cables To Avoid U.S. Surveillance*, WASH. POST (Nov. 3, 2014, 5:25 AM), https://www.washingtonpost.com/news/the-switch/wp/2014/11/03/brazil-begins-laying-its-own-internet-cables-to-avoid-u-s-surveillance [https://perma.cc/R54U-YYCK]; Richard Kemeny, *Brazil Is Sliding into Techno-Authoritarianism*, MIT TECH. REV. (Aug. 19, 2020), https://www.technologyreview.com/2020/08/19/1007094/brazil-bolsonaro-data-privacy-cadastro-base [https://perma.cc/9GHL-HV64].

47. Sarah Rainsford, *LinkedIn Blocked by Russian Authorities*, BBC NEWS (Nov. 17, 2016), https://www.bbc.com/news/technology-38014501 [https://perma.cc/ZP43-JQXM].

48. *Putin Signs Law Making Russian Apps Mandatory on Smartphones, Computers*, REUTERS (Dec. 2, 2019, 12:17 PM), https://www.reuters.com/article/us-russia-internet-software/putin-signs-law-making-russian-apps-mandatory-on-smartphones-computers-idUSKBN1Y61Z4 [https://perma.cc/9459-AC2B].

49. Victor Tangermann, *Russia Says It Will Replace Wikipedia With State-Run Site*, FUTURISM (Dec. 3, 2019), https://futurism.com/the-byte/russia-wikipedia-unreliable [https://perma.cc/9U6D-6DST].

Wikipedia just anybody could share information with the world. They want their citizens to see their government-vetted and approved information. China hasn't written its own Wikipedia, but it has effectively achieved much the same result by banning Facebook and Google unless they complied with local censorship laws, which effectively kept them out of the country. China also encouraged the development of alternatives like Baidu and Tencent, which are, because they are Chinese, ultimately beholden to the Chinese government.

It's not just China and Russia banning foreign software, though. TikTok is the most popular social media app among young people.[50] But they may not be using it for long, at least in America, because the United States is on an active campaign to shut down TikTok because it is owned by a Chinese parent company.[51] And if it's owned by a Chinese parent company, the U.S. government fears they must secretly be spying on us.[52] Now, I don't know whether TikTok is, in fact, secretly spying on us.[53] But I also don't know that we should care. I'm not sure

50. TikTok has been downloaded over two billion times. *See* Jyoti Panday, *The Hypocrisy of a U.S. TikTok Ban*, INTERNET GOVERNANCE PROJECT (July 28, 2020), https://www.internetgovernance.org/2020/07/28/the-hypocrisy-of-a-u-s-tiktok-ban [https://perma.cc/Z5DK-KEPN].

51. Drew Harwell & Tony Romm, *Inside TikTok: A Culture Clash Where U.S. Views About Censorship Often Were Overridden by the Chinese Bosses*, WASH. POST. (Nov. 5, 2019, 4:38 PM), https://www.washingtonpost.com/technology/2019/11/05/inside-tiktok-culture-clash-where-us-views-about-censorship-often-were-overridden-by-chinese-bosses [https://perma.cc/K33U-EFQH] (noting censorship concerns but also pointing out that TikTok itself is based in the United States and doesn't use Chinese moderators for its platform); Brian Fung & Jill Disis, *Trump Administration Appeals Court Order Blocking TikTok Restrictions*, CNN (Dec. 28, 2020, 9:43 PM), https://www.cnn.com/2020/12/28/tech/tiktok-federal-appeal-intl-hnk/index.html [https://perma.cc/JW5A-LL8L] (noting the Trump administration "appealed a decision handed down by a federal judge . . . that prevented authorities from fully implementing its restrictions against" TikTok).

52. *See* Neil Vigdor, *U.S. Military Branches Block Access to TikTok App Amid Pentagon Warning*, N.Y. TIMES (Jan. 4, 2020), https://nyti.ms/2Qois6N [https://perma.cc/E5YY-AT2K].

53. Many of these claims come from political rather than expert sources. *See, e.g.*, Alyza Sebenius, *TikTok App Merits National Security Investigation, Senators Say*, BLOOMBERG (Oct. 24, 2019, 9:58 AM), https://www.bloomberg.com/news/articles/2019-10-24/tiktok-app-merits-national-security-investigation-senators-say [https://perma.cc/47R4-QD8U]. The actual technical evidence of TikTok collecting data from phones was consistent with collecting data in order to block spam, and the report found that virtually every large app was doing the same thing. *See* Talal Haj Bakry & Tommy Mysk, *Popular iPhone and iPad Apps Snooping on the Pasteboard*, MYSK (Mar. 10, 2020), https://www.mysk.blog/2020/03/10/popular-iphone-and-ipad-apps-snooping-on-the-pasteboard [https://perma.cc/UW2F-YFD8]. And TikTok, unlike many U.S. apps, fixed the privacy bug when it was identified publicly. *Id*.

that if foreign intelligence agents actually saw everything Americans were doing on TikTok, they would gain much of great social value. Or perhaps the national-security apparatus cares more about our personal lives than we think. After all, the United States also barred Chinese ownership of the gay dating app Grindr on national-security grounds.[54]

TikTok and Grindr illustrate a broader point—it's not just authoritarian governments that are using balkanization to lock down the internet. The United States is responding in a number of cases by saying, "We don't want foreign apps on our soil." And it's not just TikTok; the United States has also banned WeChat, the leading Chinese communications platform and one many Americans use to conduct business with China.[55] It has prevented a Chinese company from acquiring a hotel management software company on "national security grounds."[56] And the FBI has taken the position that any mobile app from Russia is a "potential counterintelligence threat."[57]

Europe is in an interesting middle position because it doesn't really have its own software companies,[58] in part because of its less permissive attitude toward internet freedom.[59] Most of the technology companies that developed did so in the United States. But Europe is

---

TikTok collects data on its users, but note that many U.S. companies collect parallel sorts of data from their users. *Id*. TikTok may also respond to Chinese requests to censor content, but that's a different objection.

54. Jay Peters, *Grindr Has Been Sold by Its Chinese Owners After the US Expressed Security Concerns*, VERGE (Mar. 6, 2020, 1:26 PM), https://www.theverge.com/2020/3/6/21168079/grindr-sold-chinese-owner-us-cfius-security-concerns-kunlun-lgbtq [https://perma.cc/WP4N-5PJJ].

55. Ana Swanson, David McCabe & Jack Nicas, *Trump Administration To Ban TikTok and WeChat from U.S. App Stores*, N.Y. TIMES (Sept. 18, 2020), https://nyti.ms/3hIAN9l [https://perma.cc/3VFY-Y4QR].

56. David McLaughlin, *Trump Blocks Chinese Deal for U.S. Software Firm StayNTouch*, BLOOMBERG (Mar. 6, 2020, 11:49 AM), https://www.bloomberg.com/news/articles/2020-03-06/trump-blocks-chinese-deal-for-hotel-management-software-company [https://perma.cc/HQ4P-BL8Q].

57. Ben Brody, *Russian Apps Could Be 'Counterintelligence Threat,' FBI Says*, BLOOMBERG (Dec. 2, 2019, 2:00PM), https://www.bloomberg.com/news/articles/2019-12-02/russian-apps-could-pose-counterintelligence-threat-fbi-warns [https://perma.cc/JCE2-QTPY].

58. That may be changing. In response to the Trump administration and U.S. nationalism, Europe has "embarked on a generational project toward 'digital sovereignty,' mixing tougher rules against foreign tech companies with efforts to boost local innovation." Steven Erlanger & Adam Satariano, *In U.S. Tech Battle with China, Europe Feels Pinch*, N.Y. TIMES (Brussels), Sept. 12, 2020, at A10.

59. *Cf.* Josh Lerner & Greg Rafert, *Lost in the Clouds: The Impact of Changing Property Rights on Investment in Cloud Computing Ventures* (Nat'l Bureau of Econ. Rsch., Working Paper No. 21140, 2015) (showing that investment in tech innovation increased in the United States and declined in Europe because of stricter European IP rules); Hall, *supra* note 27.

by some measures the largest market in the world.[60] And as the United States increasingly abandons any pretense of global leadership, Europe increasingly controls the way U.S. companies work,[61] in several different ways. Sometimes it does so by setting a standard that others follow—passing something like the General Data Protection Regulation ("GDPR") on privacy, which then California copied in its new Privacy Act.[62] Sometimes Europe prompts balkanization within a company, demanding geoblocking—in effect saying, "We don't care what your U.S. consumers experience. Here is what everyone in Europe has to see."[63] Most problematic, sometimes it does so by insisting on imposing its rules worldwide. The GDPR rules, for instance, apply not just to European citizens, not just to transactions in Europe, but to any company that does any business with customers in Europe, which is almost any company.[64]

Anu Bradford has gone so far as to say the European Union rules the world at this point, not because it is the most powerful—although it does currently have the largest economy—but because it has the regulatory will to use that economic power to try to tell other people what they have to do, at least in Europe.[65]

Not only do people increasingly use different software and have different experiences in different countries, but even when they use the same software, it is often customized for location. And what that means increasingly is that the promise of the internet—that we get to communicate with people, we get to share information and experiences with people all around the world—is being cut short. The news you see, the facts you see, and even the maps you see change depending on where you are.[66] That may be because they're being produced by different companies. Or it may be that the same global company is

60. *EU Position in World Trade*, EUR. COMM'N (Feb. 9, 2019), https://ec.europa.eu/trade/policy/eu-position-in-world-trade/#:~:text=The%20EU%20is%20the%20largest,the%20world's%20largest%20trading%20block.&text=The%20EU%20is%20the%20top%20trading%20partner%20for%2080%20countries [https://perma.cc/CE8G-YQS8].

61. *Id.* at xiii–xiv, 99-101.

62. California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100–1798.199 (2018).

63. *See generally* Yu, *supra* note 26 (discussing geoblocking).

64. *See* Keller, *supra* note 32, at 290.

65. BRADFORD, *supra* note 30, at 25–65.

66. David Yanofsky, *See How Borders Change on Google Maps Depending on Where You View Them*, QUARTZ (June 23, 2014), https://qz.com/224821/see-how-borders-change-on-google-maps-depending-on-where-you-view-them [https://perma.cc/H7JS-5E38].

giving different information to different people in different countries because their governments demand it.[67]

B. Nationalizing Hardware Networks

But it's not just software. Increasingly, hardware is itself being nationalized. Now, some of this is market division. The iPhone is the dominant device in the United States, the United Kingdom, Canada, Australia, New Zealand, Denmark, Norway, Belgium, Switzerland, and Japan. But those are the only countries in which the iPhone is the dominant phone. In the rest of the world, some phone from the Android ecosystem is the dominant phone, and iPhone shares are actually quite small. Indeed, the iPhone has less than one-third of the overall market.[68]

That could be consumer choice—iPhones cost more than a lot of Android phones, so maybe they're more likely to be purchased in rich countries. But that's not all of it. In most of Europe, the iPhone is not dominant.[69]

The fact that different countries use different phone hardware is going to become an increasingly significant problem. The United States is currently in the process of banning Chinese phones from the market. The government views Huawei and ZTE phone technology as a security risk, much like TikTok.[70] The U.S. government is trying to keep them out of the U.S. market altogether.[71] And it is pushing

67. Facebook engages in geotargeting, for instance. *About Location Targeting*, *Business Help Center*, FACEBOOK FOR BUS., https://www.facebook.com/business/help/202297959811696 [https://perma.cc/SM8E-YAJ7].

68. *See Android v iOS Market Share 2019*, DEVICEATLAS (Sept. 9, 2019), https://deviceatlas.com/blog/android-v-ios-market-share [https://perma.cc/QVR7-3B23] (finding that most countries prefer Android); *Samsung Reclaims the Top Spot as Smartphone Market Performs Better Than Expected with 353.6 Million Device Shipments in 3Q20, According to IDC*, IDC (Oct. 29, 2020), https://www.idc.com/getdoc.jsp?containerId=prUS46974920 [https://perma.cc/D2VS-GR47].

69. *Id.* The United Kingdom is no longer in the European Union, unfortunately. *U.K. Leaves E.U., Embarking on an Uncertain Future*, N.Y. TIMES (Jan. 31, 2020), https://nyti.ms/2OggOCT [https://perma.cc/J7G7-PG7T].

70. *See* Katie Collins, *Pentagon Bans Sale of Huawei, ZTE Phones on US Military Bases*, CNET (May 2, 2018, 5:54 AM), https://www.cnet.com/news/pentagon-reportedly-bans-sale-of-huawei-and-zte-phones-on-us-military-bases [https://perma.cc/6J6Y-WU6C]; Todd Shields, *FCC Calls Huawei, ZTE Security Threats as It Bars Subsidies*, BLOOMBERG (July 1, 2020, 4:37 AM), https://www.bloomberg.com/news/articles/2020-06-30/fcc-designates-china-s-huawei-zte-as-national-security-threats [https://perma.cc/9JMP-7DUT].

71. Shields, *supra* note 70.

Europe—so far, unsuccessfully—to ban Chinese phone technology as well.[72] The United States won't even let Huawei use American technology to build its phones.[73] It grounded its entire fleet of drones because they had Chinese parts in them.[74] It has even objected to the presence of Huawei router equipment on private land sufficiently near a U.S. military base. We not only don't want Huawei phones or technology in the United States or on U.S. military bases, but we don't want them within a certain geographic range around a U.S. military base.[75] The U.S. attorney general has even proposed nationalizing (foreign) cell-phone makers to create a U.S. counterweight to Huawei.[76] There may be legitimate security concerns with Huawei phones, though there is disagreement on that score.[77] But this reaction seems quite extreme.

It's not just cell-phone makers. As part of this policy, the United States is affirmatively engaged in a mercantilist battle to try to promote Qualcomm and Qualcomm's chips over alternatives. The U.S. government filed a brief challenging the Federal Trade Commission—a different branch of the U.S. government—essentially saying, "We have to let Qualcomm hold on to a monopoly on chips, even though

72. Iain Rogers, *Pompeo Tells Germany To Tackle China or Lose Data Sharing*, BLOOMBERG (May 31, 2019, 8:25 AM), https://www.bloomberg.com/news/articles/2019-05-31/pompeo-tells-germany-to-tackle-china-or-lose-data-sharing [https://perma.cc/WHH2-BQ4D].

73. Ana Swanson, *U.S. Delivers Another Blow to Huawei*, N.Y. TIMES (Oct. 22, 2020, 11:33 AM), https://nyti.ms/3cC57QX [https://perma.cc/24K6-RQGL].

74. Well, the civilian government drones, anyway. Lisa Friedman & David McCabe, *Interior Dept. Halts Drones Over Worries About China*, N.Y. TIMES (Jan. 30, 2020), https://nyti.ms/38TvKPj [https://perma.cc/J3S9-2ZD2]. Apparently, U.S. killer drones with Chinese parts are still OK.

75. Todd Shields, Alyza Sebenius & Scott Moritz, *FCC Wants To Know if Huawei Gear Is Near U.S. Military Bases*, BLOOMBERG (Nov. 5, 2019, 2:43 PM), https://www.bloomberg.com/news/articles/2019-11-05/fcc-wants-to-know-if-huawei-gear-is-near-u-s-military-bases [https://perma.cc/WJ6P-FGH3].

76. Mark Hosenball & David Brunnstrom, *To Counter Huawei, U.S. Could Take 'Controlling Stake' in Ericsson, Nokia: Attorney General*, REUTERS (Feb. 6, 2020, 6:03 AM), https://www.reuters.com/article/-idUSKBN2001DL [https://perma.cc/SH8Z-2PA6].

77. *Compare* Angelina Rascouet, Eyk Henning, Nabila Ahmed & Thomas Pfeiffer, *Phone Firms Fearing Huawei Crackdown Say 5G Risks Are Overblown*, BNA TECH. & TELECOMM. L. NEWS (Jan. 24, 2020, 10:21 AM), https://www.bloomberglaw.com/document/X96LP4FC000000 [https://perma.cc/WR75-NA9N] (quoting executives from Verizon and Ericsson who assert 5G is more secure than its 4G and 3G predecessors), *with* Patrick Donahue, *German Spy Chief Says Huawei Can't Be 'Fully Trusted' in 5G*, BNA TECH. & TELECOMM. L. NEWS (Oct. 29, 2019, 10:59 AM), https://www.bloomberglaw.com/document/X5JTSQOK000000 [https://perma.cc/6LWG-CCHB] (noting a lack of trust due to Huawei's dependence on the Communist Party and China's intelligence apparatus).

they're violating the antitrust laws, because to do otherwise would violate national security."[78] If we let anybody but Qualcomm build the chips, the Justice Department reasoned, who knows what's going to be in those chips? They could have spyware or back doors built in that would give the Chinese government access to information passed through the chips.[79] The U.S. government has sought to block other semiconductor mergers on "national security" grounds.[80]

This isn't just an objection to Chinese technology. The Trump administration also refused to allow Broadcom to buy Qualcomm because Broadcom is based in Singapore.[81] Again, the reasoning was nationalistic. Right now, the theory seems to be, the United States would have ultimate control over Qualcomm because they're based in the United States.[82] But if they're based in Singapore, who knows what could happen? The Singaporean government could impose restrictions or requirements on what the merged company does. Conversely, and not incidentally, the United States would be less able to insert its own back doors into the chips or impose requirements.

Nor is nationalization limited to the United States and China. India has barred a variety of Chinese mobile apps, including TikTok.[83] The United States has been lobbying Europe to do the same thing, even threatening to cut off data sharing with Europe if they don't cut

78. *See* Brief of the United States of America as Amicus Curiae in Support of Appellant and Vacatur at 32–34, Fed. Trade Comm'n v. Qualcomm Inc., 935 F.3d 752 (9th Cir. 2019) (No. 19-16122).

79. *See id.*; *see also* Katie Benner, *China's Command of 5G Is a 'Danger,' Barr Says*, N.Y. TIMES, Feb. 7, 2020, at B7 ("The White House and American national security experts have said that companies including Huawei are too closely tied to the Chinese government, and that their equipment could give Chinese officials unlawful access to data and communications if networks across the world decide to use it.").

80. Saleha Moshin, David McLaughlin & Jenny Leonard, *Trump Advised To Halt Infineon Deal Amid China Security Risk*, BLOOMBERG (Mar. 6, 2020, 3:08 AM), https://www.bloomberg.com/news/articles/2020-03-05/trump-is-warned-on-security-risk-from-infineon-deal-for-cypress [https://perma.cc/MT2P-VP38].

81. Michael Leiter, Ivan Schlager & Donald Vieira, *Broadcom's Blocked Acquisition of Qualcomm*, HARV. L. SCH. F. ON CORP. GOVERNANCE (Apr. 3, 2018), https://corpgov.law.harvard.edu/2018/04/03/broadcoms-blocked-acquisition-of-qualcomm [https://perma.cc/9LRX-D8YJ].

82. Daniel Liberto, *Why Did Trump Block Broadcom's Bid for Qualcomm?*, INVESTOPEDIA (June 25, 2019), https://www.investopedia.com/news/why-did-trump-block-broadcoms-bid-qualcomm [https://perma.cc/F3K3-E5J4].

83. Maria Abi-Habib, *India Bans Chinese Mobile Apps Like Tik-Tok*, N.Y. TIMES, June 30, 2020, at B5.

off Chinese companies,[84] and it has persuaded the United Kingdom to ban Huawei.[85]

This isn't something that's going to go unanswered. If the United States says to China, "Sorry, none of your companies can participate in building phones for the next generation," or if we say to Singapore, "Sorry, none of your companies can participate in building chips to go in those phones," other countries will do something similar in response.[86]

It's not at all clear the United States would win such a competition. China is building a 5G network, and it's not just building it in China. Through the Belt and Road Initiative, it's building that network in Africa, Latin America, and Asia as well.[87] Those countries will use a 5G network that may well be incompatible with the U.S. 5G network because we are building different hardware systems that don't necessarily talk to each other.[88] And even if data can pass between the networks, it will increasingly be on software platforms that are nation specific. The United States may ban TikTok, but that doesn't mean the rest of the world will; relatively few of those two billion downloads are American teenagers.[89]

---

84. Rogers, *supra* note 72.

85. Kitty Donaldson & Thomas Seal, *UK Says Only Matter of Time Before Huawei Exits 5G Network*, BLOOMBERG (June 30, 2020, 1:13 PM), https://www.bloomberg.com/news/articles/2020-06-30/u-k-s-dowden-says-matter-of-time-before-huawei-exits-5g-network [https://perma.cc/9D2E-6FBS].

86. I don't mean to suggest that the United States is the only or the worst offender. China has been discouraging U.S. tech companies from doing business in China for many years. Paige Leskin, *Here Are All the Major US Tech Companies Blocked Behind China's 'Great Firewall*,*'* BUS. INSIDER (Oct. 10, 2019, 12:23 PM), https://www.businessinsider.com/major-us-tech-companies-blocked-from-operating-in-china-2019-5 [https://perma.cc/XRU8-R867].

87. Emily Feng, *China's Tech Giant Huawei Spans Much of the Globe Despite U.S. Efforts To Ban It*, NPR (Oct. 24, 2019, 2:30 PM), https://www.npr.org/2019/10/24/759902041/chinas-tech-giant-huawei-spans-much-of-the-globe-despite-u-s-efforts-to-ban-it [https://perma.cc/5UW9-V8TH]; Paul Nantulya, *Implications for Africa from China's One Belt One Road Strategy*, AFR. CTR. FOR STRATEGIC STUD. (Mar. 22, 2019), https://africacenter.org/spotlight/implications-for-africa-china-one-belt-one-road-strategy [https://perma.cc/YC9L-AXYV]; Zhang, *supra* note 20.

88. Benner, *supra* note 79; Nic Fildes, *Can the 5G Network Be Secured Against Spying?*, FIN. TIMES (Jan. 18, 2020), https://www.ft.com/content/423e8406-3920-11ea-a6d3-9a26f8c3cba4 [https://perma.cc/3236-EZL3] ("One of the biggest issues for the telecoms industry is the dominance of giants like Huawei, whose technology is very hardware-centric and incompatible with other vendors' technology.").

89. *See* Mansoor Iqbal, *TikTok Revenue and Usage Statistics (2020)*, BUS. APPS (Oct. 15, 2020), https://www.businessofapps.com/data/tik-tok-statistics [https://perma.cc/AT8N-M9AL]. TikTok has 500 to 800 million active users. *Id.* "Only 9% of US internet users have used TikTok, with 5% more interested in using it; this rises to 49% for teenage users." *Id.*

This incompatibility is something we used to have in the early days of cell phones—GSM versus CDMA technologies.[90] It's something we used to have in the early days of software. You couldn't actually read files from an Apple if you were on a Windows computer and vice versa. Technical incompatibility is something we've gotten away from, to everyone's benefit. It looks like we're moving back to a world where what you can see and who you can talk to is a function of what software and hardware you use. And that, in turn, increasingly will depend on where you live.

Some of this nationalism is justified by worries about foreign spying, but I think it's at least as much justified—both in the United States and in China—by a desire for domestic spying.[91] While we rightly worry about China, the United States has a pretty comprehensive electronic surveillance infrastructure in place.[92] Anybody remember Ed Snowden? We've had sufficient shocks in the world in the past five years that we kind of forgot about that one. But the United States has built and is trying to expand quite a significant electronic surveillance mechanism. The Federal Bureau of Investigation ("FBI") has, on several occasions—including, most recently, this year[93]—tried to prevent private companies within the United States from engaging in effective encryption. They've tried to block Facebook from doing end-to-end encryption on WhatsApp.[94] They have tried to force Apple to put a back door into its phone so that when something bad happens,

90. GSM refers to "global system for mobile communications," while CDMA refers to "code-division multiple access technology."

91. *See* Anupam Chander & Uyen P. Le, *Data Nationalism*, 64 EMORY L.J. 677, 738 (2015).

92. *See* Paul Farrell, *History of 5-Eyes-Explainer*, GUARDIAN (Dec. 3, 2013), https://www.theguardian.com/world/2013/dec/02/history-of-5-eyes-explainer [https://perma.cc/8CX2-LSHR]; Ryan Gallagher & Henrik Moltke, *The Wiretap Rooms: The NSA's Hidden Spy Hubs in Eight U.S. Cities*, INTERCEPT (June 25, 2018, 8:00 AM), https://theintercept.com/2018/06/25/att-internet-nsa-spy-hubs [https://perma.cc/3K2U-2RH5].

93. *See* Jon Brodkin, *Apple Cut Backup End-to-End Encryption Plans After FBI Complained*, ARSTECHNICA (Jan. 21, 2020, 12:43 PM), https://arstechnica.com/tech-policy/2020/01/apple-reportedly-nixed-plan-for-end-to-end-encryption-in-iphone-backups [https://perma.cc/LK93-JFGM].

94. *See* Zak Doffman, *U.S. May Outlaw Messaging Encryption Used by Whatsapp, iMessage and Others, Report*, FORBES (June 29, 2019, 1:35 AM), https://www.forbes.com/sites/zakdoffman/2019/06/29/u-s-may-outlaw-uncrackable-end-to-end-encrypted-messaging-report-claims [https://perma.cc/RSG2-FLVJ].

the FBI has the ability to unlock that phone.[95] That's a battle that has been going on for a long time. The few people in the room as old as me might remember the Clipper chip of 1995, which was the last time the U.S. government said, "We need to build a back door in the internet so that the FBI can see and read everything you're doing."[96]

If we are worried about foreign surveillance of our citizens on the internet, I think at most what we could say is not that we don't do it, or that we do it less, but that historically, pervasive U.S. communication software surveillance has been used in the service of a less repressive agenda here than it has elsewhere. I hope that will remain true, but I'm not sure that it will.

And at a minimum, even if you still trust your government to always do the right thing, the rest of the world doesn't. And that means that if we're going to insist on U.S. chips with U.S. surveillance built in, and China is going to insist on Chinese chips with Chinese surveillance built in, other companies and countries are not automatically going to choose the United States as the lesser of two evils.

The software differences are bad enough. But once internet hardware is country specific, this becomes harder and harder to undo. And mobile devices are built to operate with their national networks. Chinese phones work with Chinese software apps in China; U.S. phones work with U.S. software apps in the United States. It's easier. It's more logical to optimize the software for that hardware—that is, to run different, incompatible software systems because they work best with others in the same country, which is, after all, who we communicate with most of the time. We're not just experiencing different things on the same network. Increasingly, our devices may not be capable of interoperating or even seeing the same things.

C. Nationalizing the Network Itself

Even the backbone of the internet itself is not immune from balkanization. There are increasing moves by companies and internet

95. Kim Zetter, *Apple's FBI Battle Is Complicated. Here's What's Really Going On*, WIRED (Feb. 18, 2016, 1:15 PM), https://www.wired.com/2016/02/apples-fbi-battle-is-complicated-heres-whats-really-going-on [https://perma.cc/CDY3-253F].

96. *See* Tim Matthews, *The Clipper Chip: How Once upon a Time the Government Wanted To Put a Backdoor in Your Phone*, EXABEAM: INFO. SEC. BLOG (Apr. 2, 2019), https://www.exabeam.com/information-security/clipper-chip [https://perma.cc/3B3N-VLLX]. For a discussion of these proposed "exceptional-access mandates," see Alan Z. Rozenshtein, *Wicked Crypto*, 9 U.C. IRVINE L. REV. 1181, 1198–99 (2019).

service providers ("ISPs") to filter malicious sites at the domain-name-system ("DNS") level so that they are never accessible at all, even on your server system.[97] Not that you just don't see them on your device. Your corporate server never sees them either. The DNS routing system pretends that site on the internet simply doesn't exist. If you try to send a message to it, you will not get a response.

Preventing malicious sites seems like a good idea. But the definition of "malicious sites" depends on your perspective. It could be and often is cybersecurity hacking, phishing scams, and the like. But porn, or democracy in Hong Kong, or sites that encourage voting by mail, could all be viewed as malicious sites, depending on who is deciding which parts of the internet you get to see.

Other ISPs insert their own advertising for nonexistent pages. If I try to search for a page that doesn't exist, the ISP pretends there's a page there and fills it with advertising.[98] They may do the same for pages filtered off the internet. The U.S. government did the same thing when it "seized" internet domain names for alleged IP infringement, changing the pointer in the routing system to the Justice Department web site.[99] And of course, hackers try to attack the internet routing system altogether, substituting a malicious page for the one the system expects to find. All these efforts fragment the reality we see, so that what I see at rojadirecta.com is not what you see there.

Even the very backbone of the internet—this DNS routing system—is fragile and potentially subject to government manipulation. The DNS system that makes it work is literally controlled by fourteen people who hold seven sets of keys.[100] They're sort of the early blockchain. If they all agree, this must be a canonical DNS router. If someone can change that—if those computers change their DNS entry

97. *See How Does DNS Filtering Work?*, WEBTITAN (Aug. 30, 2019), https://www.spamtitan.com/web-filtering/how-does-dns-filtering-work [https://perma.cc/R4TZ-5ZJW].

98. *Cf. Advertising Policies Help: AdSense for Domains Trademark Complaint*, GOOGLE, https://support.google.com/adspolicy/answer/50003?hl=en [https://perma.cc/N3WV-VTDV] (demonstrating that Google can display ads on pages with inactive domain names).

99. *See* Nate Anderson, *Government Admits Defeat, Gives Back Seized Rojadirecta Domains*, ARSTECHNICA (Aug. 29, 2012, 4:23 PM), https://arstechnica.com/tech-policy/2012/08/government-goes-0-2-admits-defeat-in-rojadirecta-domain-forfeit-case/ [https://perma.cc/Q8NG-4XMD] (discussing examples of government IP-related domain-name seizures). Full disclosure: I represented Rojadirecta in this case.

100. Julie Bort, *The Internet Is Actually Controlled by 14 People Who Hold 7 Secret Keys*, BUS. INSIDER (Mar. 1, 2014, 6:15 PM), https://www.businessinsider.com/the-internet-is-controlled-by-14-people-2014-3 [https://perma.cc/UH92-KS9J].

or even if they start to disagree—we no longer see the same things on the internet. That's different than blocking a website. Someone with control over a DNS server can literally create their own version of the internet that everyone who relies on that server will assume is the canonical one.[101]

The internet has always been international and global. In part, though, that's an accident of history. The United States was the de facto custodian of the internet because the companies that administered the backbone happened to be located here, because it was first built here.[102] And we have traditionally been the laissez-faire country when it comes to the internet. But that effective freedom is changing. The DNS system is not officially a U.S. phenomenon. And even unofficially, our de facto control over the DNS system is shrinking. We passed control from the U.S. government to a private, nonprofit organization called the Internet Corporation for Assigned Names and Numbers ("ICANN") a couple of decades ago.

ICANN is based in the United States, so it is nominally subject to U.S. law. ICANN is a dubious custodian of DNS.[103] Most recently, it considered (and thankfully rejected) selling ".org," the nonprofit top-level domain, for $1 billion to for-profit companies who will presumably then not do anything profit making with it.[104]

But even if you thought ICANN was fine, many countries are pushing to take control of the backbone away from the United States altogether, putting it in the hands of the United Nations through the International Telecommunications Union or, more likely, giving each country control of its own top-level domain.[105] Under this approach,

---

101. *See* Lemley et al., *supra* note 12, at 34.

102. *See generally* Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts & Stephen Wolff, *Brief History of the Internet*, INTERNET SOC'Y (1997), https://www.internetsociety.org/internet/history-internet/brief-history-internet [https://perma.cc/YX8K-C6Z4] (summarizing the development of the early stages of the internet).

103. For an older but detailed analysis, see generally A. Michael Froomkin & Mark A. Lemley, *ICANN and Antitrust*, 2003 U. ILL. L. REV. 1.

104. *See* Timothy B. Lee, *ICANN Blocks Controversial Sale of .org Domain to Private Equity Firm*, ARSTECHNICA (May 1, 2020, 1:00 AM), https://arstechnica.com/tech-policy/2020/05/icann-blocks-controversial-sale-of-org-domain-to-a-private-equity-firm [https://perma.cc/NE9L-MS87].

105. Bryan Lynn, *Did the US Just 'Give Away' Control of the Internet?*, VOA LEARNING ENG. (Oct. 03, 2016), https://learningenglish.voanews.com/a/did-the-us-government-just-give-away-control-of-the-internet-to-icann/3535200.html [https://perma.cc/6DYS-97WQ]; *Some Governments Want More Control Over the Internet via ITU*, EDRI (Aug. 29, 2012), https://edri.org/our-work/edrigramnumber10-16itu-debates-internet-regulation [https://perma.cc/7937-M4GV].

the U.K. government would have control over the parts of the DNS server that point to ".uk" and the like. Doing that would make political shutdowns or diversions to alternate realities a lot easier. And indeed, various countries—including, unfortunately, the United States—have made efforts to interfere with DNS routing for political purposes. Internet shutdowns in Iran and Turkey were done by basically rerouting or turning off the outside world's access to the country's top-level domain.[106]

In the United States, nearly a decade ago, we proposed the Stop Online Piracy Act ("SOPA") and the PROTECT IP Act ("PIPA") that would have enforced U.S. copyright law by literally making the sites that infringe invisible to the world.[107] The DNS servers simply would not return a result, and any ISP would be forced to pretend to you that those sites didn't exist—not tell you they're infringing, not take down the sites, but pretend that they did not exist at all.[108]

SOPA and PIPA died because an unprecedented number of internet users rose up against it en masse to protect the internet.[109] But I'm not sure that people have the same love for the internet in 2020 that they did in 2011. The next time a government (perhaps ours) decides to divert people away from the site they tried to visit to one the government thinks they should visit, the public might not be there to stop them. And the U.S. risk comes not just from copyright owners, but from an increasingly authoritarian—and desperate—Trump administration.[110]

III. THE INTERNET IS WORTH SAVING

The result, I think, is that we're losing the internet. We're replacing it with "the splinternet," a balkanized set of computer

106. DIGITAL PLANET, *Iran Internet Shutdown Continues*, BBC (Nov. 24, 2019, 8:32 PM), https://www.bbc.co.uk/sounds/play/w3csy676 [https://perma.cc/MX6W-5QX2]; *Internet Shutdown in Turkey's Southeast Following Mayor's Detention*, TURK. BLOCKS (Oct. 26, 2016), https://turkeyblocks.org/2016/10/26/internet-shutdown-turkey-diyarbakir [https://perma.cc/J8SP-ST69].

107. Lemley et al., *supra* note 12, at 34.

108. *Id.*

109. Alex Fitzpatrick, *The Week That Killed SOPA: A Timeline*, MASHABLE (Jan. 20, 2012), https://mashable.com/2012/01/20/sopa-is-dead-timeline-january-blackout [https://perma.cc/MBX5-P9HC].

110. *See* Tom Wheeler, *Could Donald Trump Claim a National Security Threat To Shut Down the Internet?*, BROOKINGS (June 25, 2020), https://www.brookings.edu/blog/techtank/2020/06/25/could-donald-trump-claim-a-national-security-threat-to-shut-down-the-internet [https://perma.cc/MF58-CVAT].

protocols that increasingly differs by company and by country. That's not a good thing.

Now, you might not like some aspects of the internet. Some aspects of the internet are pretty horrible. Different countries may disagree about what's wrong with it. They may want to regulate it in different ways; they may want it to do different things.[111] But the internet has improved the world in all kinds of ways. Some of those are economic. The internet access industry alone generates a trillion dollars a year,[112] and that doesn't account for the commerce the internet makes possible.

The internet has also changed our lives for the better. Our phones improve our lives in ways we don't think about because we're not lost in a foreign country where we don't speak the language. We have a map that will get us where we want to go. We're not stuck on the highway with a flat tire and no way to communicate to anyone about that fact. We're not sitting in a restaurant waiting for a friend who canceled or debating some arcane fact with our friends without a device in our pocket capable of accessing all of the world's information.

For most of my lifetime, you did not take those things for granted. These are things that became available because we have access to this intersecting universe of information. Many of those benefits involve connection. They depend on the ability of systems to work together across multiple countries, across multiple languages. That's why the internet, and not a walled garden like Prodigy or CompuServe, is the thing we use today.

Balkanization means it's harder for people to share experiences across countries. Paul Ohm and Jack Goldsmith have argued that's a good thing, because we want different countries to have different rules, and those countries should be able to regulate the internet, just as they should be able to regulate any other part of their world.[113] But I think we lose something real when we splinter the internet. Doing so takes away the ability to see what the rest of the world has, how the rest of

111. *See generally* ANUPAM CHANDER, THE ELECTRONIC SILK ROAD (2013) (arguing for harmonization wherever possible but acceptance of different regional rules governing internet behavior).

112. *The Global Internet Access Market Had Total Revenues of $981.4bn in 2016*, CISION (Nov. 9, 2017, 4:04 PM), https://www.prnewswire.com/news-releases/the-global-internet-access-market-had-total-revenues-of-9814bn-in-2016-300553419.html [https://perma.cc/H7UP-EJ7C].

113. *See* JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET? ILLUSIONS OF A BORDERLESS WORLD viii (2008); Daskal & Ohm, *supra* note 36, at 21.

the world thinks, and that's a loss. I think it's a loss for everyone, but it's a particular loss for people in repressive regimes who can look to the outside world for hope, for inspiration to demand change, and for the means of facilitating that change. If we take that away by allowing repressive governments to control how their citizens see the internet, we take away the prospect of freedom for a substantial number of people.

The internet famously enabled democratic uprisings in the Arab Spring.[114] But splintering the internet also means it's easier for repressive governments to shut down outside access altogether—as Belarus,[115] Iran, and Turkey have done recently, and as India has done in Kashmir during its crackdown on minority groups. And even if they don't shut down the internet altogether, those countries will end up with much more significant control over the companies who are providing the information to you if those companies are local.[116]

The global nature of internet companies has mitigated that risk to some extent. If China wants to censor Google, Google can tell China to pound sand, and it did.[117] Medium can tell Malaysia to pound sand, and it did when it was told to censor content that Malaysia didn't like.[118] Baidu can't do the same with China because Baidu is in China. And an Iranian-based internet company or a Russian version of Wikipedia shouldn't be expected to offer much resistance to the demands of the nations where they are based.[119]

---

114. Anupam Chander, *Googling Freedom*, 99 CALIF. L. REV. 1, 3 (2011) ("Across the world, dissidents have used the web to circulate information, relying on offshore servers to avoid local repression.").

115. *See* Ryan Gallagher, *Belarusian Officials Shut Down Internet with Technology Made by U.S. Firm*, BLOOMBERG (Aug. 28, 2020, 7:22 AM), https://www.bloomberg.com/news/articles/2020-08-28/belarusian-officials-shut-down-internet-with-technology-made-by-u-s-firm [https://perma.cc/UTH4-SW2M].

116. Chander & Le, *supra* note 91, at 735 ("The end result of data localization is to bring information increasingly under the control of the local authorities . . . .").

117. Kaveh Waddell, *Why Google Quit China – And Why It's Heading Back*, ATLANTIC (Jan. 19, 2016), https://www.theatlantic.com/technology/archive/2016/01/why-google-quit-china-and-why-its-heading-back/424482 [https://perma.cc/3PG5-BNBS] (discussing Google's decision to withdraw from China in 2010).

118. *Why Has Malaysia Blocked Medium?*, ENGADGET (Jan. 28, 2016), https://www.engadget.com/2016-01-28-malaysia-medium-block-explainer.html [https://perma.cc/4NJC-5BBV].

119. Some, but not all, U.S. companies pushed back against unlawful surveillance by the U.S. government during the Bush and Obama administrations. Elias Groll, *How American Companies Enable NSA Surveillance*, FOREIGN POL'Y (Oct. 4, 2016, 4:40 PM), https://foreignpolicy.com/

Nationalized surveillance-enabled systems aren't just enabling government repression. They're also a cyber-security nightmare. Collect all of the sensitive data about what people are saying, what they're doing, what their accounts look like in a government system, and that government system will be hacked. I guarantee it. The more valuable the data the government collects, the bigger the target its database will be. And we've built not just our political and our social polity and conversation into the internet, we've built many of our most important systems around the internet backbone. Your banks, your power companies, various things that we depend on for the infrastructure of modern civilization are built into a network that we are increasingly making a nationalized, hackable, surveilled system. And the idea that governments—U.S. or foreign—will have more control over them is troubling.

The worst thing to me about the splintering of the internet is that I think the way we're losing the internet parallels the way we're losing the project of globalization. Globalization sometimes gets a bad rap,[120] but for me, it is something valuable. And we are replacing globalization with a particularly authoritarian form of tribalism in countries around the world: in the United States, the United Kingdom, China, Russia, India, Brazil, Turkey, Hungary, and the Philippines.[121] In country after country, the future seems to lie not in reaching out and interacting with the world around you, but in autarkies. Countries are drawing boundaries around their race, their nationality, their religion, and so forth. The splintering of the internet reflects that retreat from globalization, but it may also make it harder to undo. One possible mechanism for unifying the internet—international law and international norms—seems less promising than it would be in a world that was more committed to cooperation. And the results may be catastrophic.[122]

2016/10/04/how-american-companies-enable-nsa-surveillance [https://perma.cc/W8JT-AB8X]. But the United States is (hopefully still) not a repressive government.

120. John Rennie Short, *Column: Why There's a Backlash Against Globalization and What Needs To Change*, PBS (Nov. 30, 2016, 5:36 PM), https://www.pbs.org/newshour/economy/column-theres-backlash-globalization-needs-change [https://perma.cc/J5S8-SLBK].

121. *See, e.g.*, Martin Wolf, *The Rise of the Populist Authoritarians*, FIN. TIMES (Jan. 22, 2019), https://www.ft.com/content/4faf6c4e-1d84-11e9-b2f7-97e4dbd3580d [https://perma.cc/6636-GUWJ].

122. *See generally* JEFFREY A. FRIEDEN, GLOBAL CAPITALISM: ITS FALL AND RISE IN THE TWENTIETH CENTURY (2007) (arguing that a populist retreat from global trade at the beginning of the twentieth century eliminated the shared interests that otherwise staved off war, leading to World War I, World War II, and the Cold War).

IV. WHAT CAN WE DO?

That brings me to the last part of the speech, the part where I tell you how to solve the problem. Unfortunately, I don't have great ideas. Nonetheless, here are four suggestions.

First, we should promote technologies that are resilient to government censorship. End-to-end encryption of phones and messaging is a good start. We ought to be building it into all of our systems, and we ought to be using systems only if they are, in fact, encrypted. Encryption and blockchain-based technologies can allow persistent pseudonymity, so that people can actually interact with a verifiable person without having to identify them and know who they are.[123] VPNs—or "Virtual Private Networks"—can allow tunneling through national firewalls to give you access to other people's internet experiences.[124] We need to protect and promote these technologies, not undermine them. People can use them to avoid censorship in countries that engage in software filtering.[125] That means we need to fight government efforts to introduce back doors wherever we can, not just when China imposes them, but when the United States tries to impose them on Apple phones as well.

Right now, many of these technologies are fringe. If you use blockchain—or peer-to-peer networks, back in the day—the assumption is that there's probably something wrong with you. Maybe you're a drug dealer or you're engaged in copyright piracy or something. We often associate these fringe technologies with criminals, simply because we haven't developed a mainstream tradition of using them. And without widespread legitimate use, much of the early use of these technologies is indeed by criminals.[126]

But that conclusion isn't inevitable. The same thing was once said of secured-sockets-layer ("SSL") encryption. Indeed, the United States tried to block encryption from being built into the internet back

123. *Block Chains Aren't Anonymous. But They Can Be*, LEDGEROPS, https://ledgerops.com/blog/blockchains-arent-anonymous-but-they-can-be-05-01-2019 [https://perma.cc/D6J8-SU66].

124. Paul Ohm refers to VPNs as a technology of balkanization, Daskal & Ohm, *supra* note 36, at 20, but I think, in practice, that has it backwards—it is a technology that allows many to evade censorship by skirting geoblocking restrictions.

125. VPNs may have a harder time getting around a coming regime of hardware surveillance.

126. Sean Foley, Jonathan R. Karlsen & Tālis J. Putniņš, *Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies?*, 32 REV. FIN. STUD. 1798, 1800 (2019).

in 1995.[127] Now it's standard. You wouldn't want to give your credit card number to somebody, much less bank with them, if they didn't actually have a secure transaction with robust encryption. What was once considered a dangerous fringe technology that was going to allow criminals to get away with all sorts of stuff is now something so standard that we get nervous if a website doesn't have it. The same could turn out to be true of end-to-end encryption or blockchain if mainstream sites adopt them widely enough.

Widespread adoption of these technologies of connection makes balkanization harder. And at a minimum, countries that hope to protect the internet shouldn't be making them illegal, either directly or through regulation via indirect devices like copyright anticircumvention.[128] The law should resist the inference that you're facilitating a bad act by being anonymous or encrypted, and so we need to stop you. Unfortunately, the U.S. government often takes that position, and it has restricted the deployment of freedom-enhancing technologies like end-to-end encryption.[129]

Second, individuals ought to resist hyper-personalization in the private market. We ought to be troubled by device and software specialization by private companies for some of the same reasons we resist balkanization by countries. Google, Tencent, Apple, and others want to keep you in their ecosystem.[130] They want to send you from their search engine to their pet systems, their apps, and their devices, because the longer they can keep you in the ecosystem, the more information they can learn about you and the more opportunities they have to sell you things. So they are closing Applications Programming Interfaces ("APIs") and making it harder for independent companies to write software that works with their ecosystems.[131]

---

127. *See* Steven Levy, *Battle of the Clipper Chip*, N.Y. TIMES (June 12, 1994), https://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html [https://perma.cc/YL5J-XLSU] (discussing concerns about the effort to surveil communications online via the Clipper Chip); Matthews, *supra* note 96 (discussing the Clipper Chip).

128. *Cf.* 17 U.S.C. § 1201 (2018) (establishing liability for circumventing access restrictions on copyrighted works).

129. *See* Brodkin, *supra* note 93.

130. *See* Chris Hoofnagle, Aniket Kesari & Aaron Perzanowski, *The Tethered Economy*, 87 GEO. WASH. L. REV. 783, 839–40 (2019) (noting that Amazon, Apple, and Google all offer exclusive access to products in their ecosystem to those who use their home speaker products).

131. Daskal & Ohm, *supra* note 36, at 20 ("[T]he Internet has been horribly Balkanized by corporations at the app layer."); Chinmayi Sharma, *Concentrated Digital Markets, Restrictive APIs, and the Fight for Internet Interoperability*, 50 U. MEM. L. REV. 441, 442 (2019)

Venture outside. Don't use software only from your country. Don't use software all from the same company. Resisting the walled gardens at the private level helps preserve the internet and prevents it from devolving back into AOL or Compuserve.

Third, the law should promote interoperability across walled gardens. One way to do this is to encourage open APIs both as a business and a legal matter. Another way is open-source or free software. The law shouldn't mandate free software, but it should allow what Cory Doctorow calls "adversarial interoperability."[132]

Companies want to create walled gardens. They want to regulate who can see in over the wall, who can get access to that information. The law has not traditionally let them,[133] but a number of legal tools, including the Computer Fraud and Abuse Act and copyright law, have been used increasingly to try to prevent interoperability.[134] Those laws threaten to prevent competitors from making a software program that,

("[Unfortunately, these] platforms have begun closing off access to information and features by restricting APIs.").

132. *See* Cory Doctorow, *Adversarial Interoperability*, ELEC. FRONTIER FOUND. (Oct. 2, 2019), https://www.eff.org/deeplinks/2019/10/adversarial-interoperability [https://perma.cc/2Y6G-WNR8].

133. *See, e.g.*, DSC Commc'ns Corp. v. DGI Tech. Inc., 81 F.3d 597, 601 (5th Cir. 1996); Bateman v. Mnemonics, Inc., 79 F.3d 1532, 1539 n.18 (11th Cir. 1996); Lotus Dev. Corp. v. Borland Int'l, Inc., 49 F.3d 807, 821 (1st Cir. 1995) (Boudin, J., concurring), *aff'd*, 516 U.S. 233 (1996); Sega Enter. v. Accolade, Inc., 977 F.2d 1510, 1527–28 (9th Cir. 1992); Atari Games Corp. v. Nintendo of Am. Inc., 975 F.2d 832, 843–44 (Fed. Cir. 1992); Vault Corp. v. Quaid Software Ltd., 847 F.2d 255, 270 (5th Cir. 1988); Mitel Inc. v. Iqtel Inc., 896 F. Supp. 1050, 1054–55 (D. Colo. 1995); Julie E. Cohen, *Reverse Engineering and the Rise of Electronic Vigilantism: Intellectual Property Implications of "Lock-Out" Programs*, 68 S. CAL. L. REV. 1091, 1096 (1995); Pamela Samuelson, *Functionality and Expression in Computer Programs: Refining the Tests for Software Copyright Infringement*, 31 BERKELEY TECH. L.J. 1215, 1297 (2017); Joseph P. Gratz & Mark A. Lemley, *Platforms and Interoperability in* Oracle v. Google, 31 HARV. J.L. & TECH. 603, 605 (2018) ("Software copyright law has long favored interoperability. In many cases it has done so by denying protection altogether to elements of computer programs that exist only for purposes of interoperability, like APIs."). *See generally* JONATHAN BAND & MASANOBU KATOH, INTERFACES ON TRIAL: INTELLECTUAL PROPERTY AND INTEROPERABILITY IN THE GLOBAL SOFTWARE INDUSTRY (1995) (discussing the court fights over interoperability). Still other courts have found interoperability to be fair use. *See, e.g.*, Sega Enter. v. Accolade, Inc., 977 F.2d 1510 (9th Cir. 1992), *amended by* 1993 U.S. App. LEXIS 78 (9th Cir. Jan. 6, 1993); Sony Comput. Ent., Inc. v. Connectix Corp., 203 F.3d 596, 599 (9th Cir. 2000).

134. *See generally* Google v. Oracle, 886 F.3d 1179 (Fed. Cir. 2018) (adopting a broad reading of copyright to prevent interoperability); United States v. Van Buren, 940 F.3d 1192 (11th Cir. 2019) (adopting a broad reading of CFAA); Jonathan Mayer, *Cybercrime Litigation*, 164 U. PA. L. REV. 1453 (2016) (discussing the abuse of the CFAA). The Supreme Court at this writing is set to consider the scope of the Computer Fraud and Abuse Act, Van Buren v. United States, No. 19-783 (U.S. 2020), and the permissibility of interoperability in software copyright, Google v. Oracle, No. 18-956 (U.S. 2019).

say, allows Facebook users to share their data across Facebook and other platforms. That preserves incumbents by making it harder to build an alternative to Facebook. That is especially true in markets with significant network effects.[135]

Now, there are arguably good reasons why you want to prevent some sharing of data from incumbent platforms. One justification is privacy—people don't necessarily want the data they share with Facebook passed on to other companies without Facebook's consent.[136] Although I have to say that the idea that Facebook is out there protecting your privacy by preventing you from using a cross-platform app—which they successfully did in *Facebook, Inc. v. Power Ventures, Inc.*[137]—is a bit far-fetched to me.

But lack of open interfaces means concentration of private economic power. It means we all end up having to choose a single system. And in a market with strong network effects, that generally means all or most of us use the same system. And that, in turn, creates a central choke point governments can target.

That leads me to my fourth recommendation, which is we ought to be looking for mechanisms to promote vibrant competition in internet platforms. As Andrew McCreary and I explain in our paper, "Exit Strategy,"[138] we no longer see the sort of Schumpeterian competition that has driven the tech industry for the last several years, in which one company comes out of nowhere and displaces the dominant market company. That used to be a central feature of technology markets, but it hasn't happened for a long time. If you look at the dominant companies—Google, Facebook, Apple, Amazon, Netflix—none of them are less than fifteen years old.[139] Most of them

135. *See* Mark A. Lemley & Andrew McCreary, *Exit Strategy*, __ B.U. L. REV. __ (forthcoming 2021) (manuscript at 60–62), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3506919 [https://perma.cc/5RFT-GFX5]; Thomas Kadri, *Digital Gatekeepers*, 99 TEX. L. REV. (forthcoming 2021) (manuscript at 34), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3665040 [https://perma.cc/UM5T-HVZX]).

136. For a sophisticated discussion of how to balance privacy and cybersecurity with data portability and interoperability, see Peter Swire, *The Portability and Other Required Transfers Impact Assessment (PORT-IA): Assessing Competition, Privacy, Cybersecurity, and Other Considerations* (May 14, 2020) (unpublished manuscript) https://peterswire.net/wp-content/uploads/PORT-IA.Swire_.March-27-2020.pdf [https://perma.cc/5F8Q-E2SB].

137. Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058 (9th Cir. 2018).

138. Lemley & McCreary, *supra* note 135 (manuscript at 4).

139. *Id*.

are more than twenty years old. That's a long time to be dominant in the notoriously fast-moving tech industry.

We argue in Exit Strategy that we can trace this stalled competition to the venture-capital model we used to fund the tech industry. Venture capitalists fund companies with the intention of cashing out sooner rather than later. While thirty years ago that cash out generally involved an IPO that kept the startup in the market, today most startup exits involve selling the company. And increasingly those sales are to dominant incumbents. We are encouraging founders not to build their company into the new Google killer, but to sell out and to sell out to the incumbents—to Google itself.[140] We argue that we need more robust antitrust law restricting mergers. We also need to rethink the way we fund startups and reorient them toward competition rather than selling out to incumbents.[141]

But whatever the reason we have lost it, we need competition in platforms. Competition is a good thing in itself. It produces better and cheaper services. But ironically, a more fragmented market may produce a more robust internet. Without competition—without choice—it becomes much easier to think of your internet provider as your regulator, insisting that the government compel them to control speech on their platform. Bigger, older companies may be more likely to comply with even unlawful or unreasonable government requests; they have more to lose by resisting the government. And it is easier for governments to regulate a single, central platform than decentralized technologies.

CONCLUSION

The genius of the internet is that because it is global and decentralized, there is more communication of information from more sources. The internet has brought us far more creativity from far more sources than ever before. And the reason is precisely because it wasn't the information superhighway, because it was not just canonical providers of information that the rest of us passively consumed. On the internet, the providers of information are all of us. It's everybody who posts on YouTube. It's everybody who posts on a blog. The internet made all of us creators. That's got some downsides. There's a lot of misinformation out there. There's a lot of political polarization that

140. *Id.* (manuscript at 5–7).

141. *See id*. (manuscript at 8).

arguably can be traced to letting a bunch of people talk who were otherwise keeping quiet. But the internet gives us more access to information, and it gives us the tools to learn more and to try to figure out more easily what's right and what's not. It is the world's access to multiple different sources of information and content that is at stake with the splintering of the internet.

I don't think any of my suggestions are going to get us Barlow's free and independent internet. It probably never existed. But the internet took off in the 1990s as an alternative to the official government-corporate information superhighway. The idea of five hundred channels of TV is a push medium with top-down control. The internet was an insurgent, decentralized, interoperable network with no one in charge. And it was a runaway success. We got the five hundred channels, but we got a lot more. I think we should fight hard not to give up the internet for an information superhighway, particularly one that's controlled by our national governments.