DEBATE: WE NEED TO PROTECT STRONG NATIONAL BORDERS ON THE INTERNET*

DEBATE BETWEEN JENNIFER DASKAL** AND PAUL OHM,***
MODERATED BY PIERRE DE VRIES****

SILICON FLATIRONS CENTER
BOULDER, COLORADO
FEBRUARY 11, 2018

The dream of a globally interconnected Internet, pursuant to which information and data flow freely without regard to national borders, has long captured the imagination of human rights activists, business leaders, and Internet enthusiasts alike. But it is a dream that may be fading. Increasingly, and for a variety of different reasons, countries around the world have proposed or enacted laws that would increase what is known as "Internet Balkanization."[1] *Russia has enacted data localization rules that require cloud and platform providers to store data about its citizens within its physical territory.*[2] *India requires all communications*

* This debate has been edited for publication. This conversation occurred at the Silicon Flatirons Regulating Computing and Code Conference at the University of Colorado Law School on February 11, 2018. For a video of the debate, see Silicon Flatirons, *Sunday Debate: We Need to Protect Strong National Borders on the Internet?*, YOUTUBE (Feb. 12, 2018), https://youtu.be/Ig_6RAHANsY [https://perma.cc/V4BS-YQRL].

** Jennifer Daskal is an Associate Professor of Law at American University Washington College of Law, where she teaches and writes in the fields of criminal, national security, and constitutional law. From 2009 to 2011, Daskal was counsel to the Assistant Attorney General for National Security at the Department of Justice.

*** Paul Ohm is a Professor of Law at the Georgetown University Law Center. He specializes in information privacy, computer crime law, intellectual property, and criminal procedure. He serves as a faculty director for the Center on Privacy and Technology at Georgetown.

**** Pierre de Vries is an Executive Fellow of the Silicon Flatirons Center at the University of Colorado, Boulder, and Co-Director of its Spectrum Policy Initiative. He is a Visiting Senior Scientist at the Institute for Networked Systems of RWTH Aachen University and serves on the FCC Technology Advisory Council. His current work focuses on maximizing the value of radio operation by modeling and managing inter-system interference.

[1] *See, e.g.*, Jonah Force Hill, *The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders,* LAWFARE RES. PAPER SERIES, July 21, 2014, at 3–5.

[2] *See* William Alan Reinsch, *A Data Localization Free-for-All?*, CTR. FOR STRATEGIC & INT'L STUD. (Mar. 9, 2018), https://www.csis.org/blogs/future-digital-trade-policy-and-role-us-and-uk/data-localization-free-all [https://perma.cc/UM2B-XK33].

between users in India to be stored in India.[3] *The European Union places strict data protection controls on the transfer of information about their residents to other countries.*[4] *These are just a handful of the many examples worldwide.*

On February 11, 2018, at the flagship conference of the Silicon Flatirons Center at the University of Colorado, two scholars of technology law debated Internet Balkanization. Paul Ohm, of Georgetown University Law Center, offered the motion and bore the burden of persuasion on the proposition: "We need strong national borders on the Internet." Opposing the motion was Jennifer Daskal of the American University Washington College of Law.

The following is a transcript of the debate, lightly edited by the participants to clarify arguments and provide citation for factual propositions. The debate was moderated by Silicon Flatirons Executive Fellow Pierre de Vries, who opened the debate by polling the audience.

Pierre: And so the purpose of the debate is to see whether you change your mind from now until after you've heard the arguments from the two sides. So, we'll keep this poll open for five minutes, and then we'll close it, and you won't be able to vote anymore. And then you'll vote again, at the end. So, why don't we start and kick it off—over to you, Paul.

Poll Statement: "We need to protect strong national borders on the Internet."

Poll Results: Agree – 32.9%; Disagree – 67.1%.

Paul: Thank you all. Hearing this man with his classic British accent talking about Oxford-style debates makes me nervous. I'm not quite sure what that means. I did, just in case, pack the only thing I know about Oxford, namely, I have a wand and a [robe][5] in my suitcase, and I want the crowd to know that I'm a proud Hufflepuff. That is Oxford I'm thinking of, isn't it?

Pierre: Is it dark blue or light blue?

[3] *See id.*

[4] *See* Mike Hintze, *Data Controllers, Data Processors, and the Growing Use of Connected Products in the Enterprise: Managing Risks, Understanding Benefits, and Complying with the GDPR*, 22 J. INTERNET L. 17, 22–23 (2018).

[5] [Paul Ohm] — In the debate, I used the word "cape" here, to my everlasting shame.

Paul: See, I have no idea what you're talking about. I am ill-equipped to be doing this.

Let me start by noting the passing, four days ago, of John Perry Barlow.[6] I did not know him personally, but a lot of people I know both knew and loved him. He was a lyricist for the Grateful Dead (and I know nothing about the Grateful Dead either) who came into my consciousness when he wrote a remarkable document called, *A Declaration of Independence of Cyberspace*.[7] Many in the room have read it, and even if you haven't read it, you've been influenced by it. Everyone who works in technology policy has felt the influence of this document.

Barlow wrote the Declaration of Independence of Cyberspace twenty-two years ago, in 1996. Because I am so much older than the students in attendance, I remember what 1996 meant for the Internet. At that time, in the halcyon days just before the dotcom bust, the Internet seemed like a magical, shared experiment in global interconnectivity. Barlow captured this optimism in this proclamation. The opening paragraph is probably what is most well-known. "Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather."[8]

This was a well-written and stirring call to independence on behalf of the users of the world, impelling them to recognize that the ability to engage in frictionless and seamless communication with anybody on the globe was the dawn of something new to the planet. Whatever that new thing was, it fueled a heady libertarianism, liberating us from the governments that had kept us down in the past.

In the twenty-two-year arc between when those words were written to today, the next relevant touch point occurred in 2007, when legal scholars Tim Wu and Jack Goldsmith wrote, *Who Controls the Internet: Illusions of a Borderless*

[6] Sam Roberts, *John Perry Barlow, 70, Dies: Champion of an Open Internet*, N.Y. TIMES, Feb. 8, 2018, at B14.

[7] John Perry Barlow, *A Declaration of Independence of Cyberspace*, ELECTRONIC FRONTIER FOUND. (Feb. 8, 1996), https://www.eff.org/cyberspace-independence [https://perma.cc/Y25C-GUBT].

[8] *Id.*

World.[9] Writing after a decade's worth of experience upon which to test the vision of Barlow, Wu, and Goldsmith, concluded that, contrary to Barlow's libertarian vision, the weary, terrestrial governments of yore, had become quite active and capable of regulating the "new home of mind," the Internet.[10]

The debate between Barlow, on the side of the Internet as liberation from government, and Goldsmith and Wu, on the controllability of the Internet by government, has never ceased over the lifetime of the Internet. We return to it today, in the form of the proposition put before you, which I am to defend: we need to protect strong national borders on the Internet. I will argue in three steps in support of the proposition.

The first step in my argument is the proposition that the Internet today is terrible. In step two, I will point out the many ways in which the Internet is already Balkanized.[11] In fact, the Internet has probably never been the purely interconnected global network that we have long imagined and spoke about. That's mythmaking and fiction. Certainly, it is not seamless and interconnected today. Finally, step three, and this is where I think I bear the most burden: the benefits of increased, localized regulation of the Internet would outweigh the costs in many cases. Let me elaborate on these three steps.

Step one, the Internet is terrible. It is a horrible, horrible, horrible place, especially compared to our shared dreams of 1996. By the way, Vint Cerf, who is sitting a few feet from me in the front row of the audience, just blew a raspberry at me when I said the Internet is terrible. That just might be a highlight of my career.

Before the start of the conference, I thought this would be a much more difficult proposition to support, but the

[9] JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET?: ILLUSIONS OF A BORDERLESS WORLD (2006).

[10] *See id.* at 44–68.

[11] At least, in theory, the Internet is the globally connected "network of networks" that uses the TCP/IP protocols to communicate. Any connected device on the Internet should be reachable, in theory, by any other device. Kevin Werbach, *The Centripetal Network: How the Internet Holds Itself Together, and the Forces Tearing It Apart*, 42 U.C. DAVIS L. REV. 343, 373–74 (2008). The term "Internet Balkanization" refers to changes that might be made that would segment the Internet into different pieces, with borders that might mirror borders on the physical globe, so that some devices will not be able to reach others, due to technical incompatibility, legal prohibition, physical separation, or some combination of these. *Id.* at 353–54.

terribleness of the Internet has essentially been the theme of the day. I think a form of this conclusion has been uttered by almost every speaker on almost every panel today, well maybe except by the guy from T-Mobile; he loves the way the Internet is working for him today.[12]

Let me count only some of the ways the Internet is terrible. The predominant business model of this network we've devised asks us to share our secrets to giant platforms that they turn around and sell to advertisers for micro pennies.[13] The users of the Internet are the natural resource that is being mined by these corporate globalists to extract this value from us.[14]

Also, much of the Internet today has become just a giant television network with a million channels. What used to be about two-way communication and discourse has largely devolved into the passive reception of audio and video images.

The next way the Internet is horrible is insecurity. Vint Cerf started the day talking about the intrinsic problems that impede attempts to secure this broken, insecure network.[15]

Finally, we get to problems that are of a more important, human order. These include fake news, filter bubbles, harassment, threats, and discrimination. In short, the Internet today has not become the font of generativity that Barlow had in mind. In this world, no longer is everything possible. Instead, a small number of corporate superpowers decide what the rest of us get to do. They get to shape who we are and what we become.

Step one brings me at last to the proposition for this debate: I am supporting the claim that we need new laws that protect strong borders on the Internet. Perhaps the only good remaining way to address some of the terribleness of

[12] Jeffrey Binder, Executive Vice President Home & Entertainment of T-Mobile USA, Inc., was on a panel titled "Challenges of Governance" earlier at the Silicon Flatirons conference. For a video of that panel, see Silicon Flatirons, *Sunday: Challenges of Governance*, YOUTUBE (Feb. 11, 2018), https://youtu.be/XvjbVpWSObE [https://perma.cc/2JK8-BN8A].

[13] *See* JOSEPH TUROW, THE DAILY YOU: HOW THE NEW ADVERTISING INDUSTRY IS DEFINING YOUR IDENTITY AND YOUR WORTH 7 (2011).

[14] *See* Julie E. Cohen, *The Biopolitical Public Domain: The Legal Construction of the Surveillance Economy*, 31 PHIL. & TECH. 213, 213–14 (2017).

[15] *See* Vint Cerf, *Keynote Address: The Battle for a Safer Internet*, 17 COLO. TECH. L.J. 1 (2018); Silicon Flatirons, *Sunday: Introduction and Keynote*, YOUTUBE (Feb. 12, 2018), https://youtu.be/atWFGNlmiKg [https://perma.cc/E4JZ-A6PN].

today's Internet is through laws like Brazil's failed proposal to mandate data localization.[16] In these debates, this is often smeared with the scary label Internet Balkanization. My burden is to try to convince you that data localization and Internet Balkanization aren't as bad as they are made out to be, and they might be the only way to fix what is broken online.

As an aside, we should feel extremely nervous about the state of the debate about localization and Balkanization. It appears that there is not a respectable, authoritative person in the United States who can say anything good about data localization. Data localization has inspired commentary by the U.S. Chamber of Commerce,[17] the Electronic Frontier Foundation (EFF),[18] and academics of every stripe,[19] people who have never all agreed on a single thing, not about copyright, net neutrality, privacy, or innovation policy. But on this topic, they all agree with the shared conclusion that data localization would not only be the death of the Internet as we know it; it probably would cause Armageddon, at least if you're to believe the tenor of the arguments we've heard. The one-sided nature of this discourse, the fact that the argument against localization almost goes without saying, should make us all extremely nervous. Today, I volunteer to be that guy, the one American who's going to say something good about Balkanization and data localization.

Step two, one reason not to fear Balkanization is that the Internet is already Balkanized and has been so for a long time. Let's start where most of my opponents would start: with the governments that we recognize in this world as

[16] Data localization laws would obligate companies with users in a given country to store all of the information about those users within the physical boundaries of that country. Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 EMORY L.J. 677, 683–85 (2015).

[17] *See* Rich Cooper, *Say No to the Balkanization of the Internet*, U.S. CHAMBER COM. FOUND. (March 30, 2015), https://www.uschamberfoundation.org/blog/post/say-no-balkanization-internet/42923 [https://perma.cc/LMG5-342Y].

[18] *See* Letter from Am. Civil Liberties Union et al., to Patrick J. Leahy, Chairman, U.S. Senate, & Jeff Sessions, Ranking Member, U.S. Senate (Oct. 26, 2010) [hereinafter *Letter from Human Rights Advocates*], https://www.eff.org/files/filenode/coica_files/coica_human_rights_letter.pdf [https://perma.cc/6Q67-AFTC].

[19] *See, e.g.*, JONAH FORCE HILL, INTERNET FRAGMENTATION: HIGHLIGHTING THE MAJOR TECHNICAL, GOVERNANCE AND DIPLOMATIC CHALLENGES FOR U.S. POLICY MAKERS (2012); Ido Kilovaty, *"Balkanization" of the Internet as a Response to Cybersecurity Threats: A Viable Solution or a Serious Obstacle for the Future of the Net?*, CYBER F.: CYBER BLOG (May 11, 2015, 1:39 PM), http://weblaw.haifa.ac.il/he/Research/ResearchCenters/cyberforum/cyberblog/Lists/Posts/Post.aspx?ID=13 [https://perma.cc/WV9M-HWFB]; Sascha Meinrath, *The Future of the Internet: Balkanization and Borders*, TIME (Oct. 11, 2013), https://wp.me/p1RTSY-aPw [https://perma.cc/N9KM-KGLP].

either outright totalitarian, or at least not fully embracing democratic values. China, Russia, Bahrain, and Saudi Arabia, for many years, have engineered central points of control and failure into communications networks.[20] You can look elsewhere throughout the Middle East for different places where the first way to respond to unrest from the populace, is to shut down the providers and social networks.[21] This kind of control has been there from the start.

But the story of today's Balkanized Internet covers more democratic nations and western nations too. The European Union recognizes the Right of Erasure, or "Right to be Forgotten," which means that there are capabilities which European citizens enjoy that Americans do not.[22] Germany has enacted extreme strictures on hate speech, including a relatively new law that has attracted a lot of attention.[23] The surveillance capability of the nation's government is Balkanized, as evidenced by the case now pending in the Supreme Court between the United States and Microsoft about the global reach of an American search warrant when delivered on an ISP in the United States about data that's stored in Ireland.[24]

[20] *See* GOLDSMITH & WU, *supra* note 9, at 73–75.

[21] *See* ZEYNEP TUFEKCI, TWITTER AND TEAR GAS: THE POWER AND FRAGILITY OF NETWORKED PROTEST 227 (2017).

[22] The "Right to be Forgotten" was first recognized as an enforceable right under the European Union's Data Protection Directive. Council Directive 95/46, art. 12(b), 1995 O.J. (L 281) 42; *cf.* Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, 2014 E.C.R. 317, ¶ 99 (holding that the Data Protection Directive creates a presumption that search engine operators must delete links to a data subject's personal information from search results at the request of that data subject, unless there is a "preponderant interest of the general public in having . . . access to the information"). It has since been expressly enshrined into law in the successor to the Directive, the General Data Protection Regulation. Council Regulation 2016/679, art. 17, 2016 O.J. (L 119) 43, 44 [hereinafter GDPR] ("The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay . . . ."). Whatever the name, the right means individuals can demand that database owners and online services delete truthful information about them, once the information is no longer needed or of immediate relevance. Meg Leta Jones, *A Digital Dark Age and the Right to Be Forgotten*, 17 J. INTERNET L. 1, 11 (2013) ("The right to be forgotten has been described as 'the right to silence on past events in life that are no longer occurring.'" (quoting Gorgio Pino, *The Right to Personal Identity in Italian Private Law: Constitutional Interpretation and Judge-Made Rights*, *in* THE HARMONIZATION OF PRIVATE LAW IN EUROPE 225, 237 (M. Van Hoecke & F. Ost eds., 2000))).

[23] Netzwerkdurchsetzungsgesetz [NetzDG] [Network Enforcement Act], Sept. 1, 2017, BUNDESGESETZBLATT, Teil I [BGBL I] at 3352, 3355, art. 3 (Ger.); Natasha Lomas, *Germany's Social Media Hate Speech Law Is Now in Effect*, TECHCRUNCH (Oct. 2, 2017), https://techcrunch.com/2017/10/02/germanys-social-media-hate-speech-law-is-now-in-effect/ [https://perma.cc/W38M-UCS8].

[24] After we held this debate, but before publication, Congress passed and the President signed the Clarifying Lawful Overseas Use of Data Act (CLOUD Act), as part of a larger spending package. *See* Consolidated Appropriations Act, Pub. L. No. 1115-

> Corporations have Balkanized the Internet as well. Here is a list of Balkanizing technologies that were either not very widespread or didn't exist at the time that Barlow wrote: Network Addressed Translation, VPNs, corporate LANs, the "dark net," and content delivery networks. These are all technologies that have made the dream of sending a packet from Delhi and having it arrive at an arbitrary computer in Bogota less than a guaranteed thing. We transit less of a fully connected network graph than we once did.
>
> Finally, the Internet has been horribly Balkanized by corporations at the app layer. Companies increasingly engineer interconnectivity out of their applications, trying hard to capture users in a single platform subject only to their control. Facebook does not want its users' status updates to be easily reproducible in bulk to Twitter, much less the valuable social graph of relationships between users.[25] Google refuses to share information about who clicked what in response to a search query with competitors like Bing or Duckduckgo.[26] It was not always so. An earlier Internet supported a freer interchange of information, even between competitors.
>
> One example is in the rise and fall of the API, or Application Programming Interface. APIs represented an act of remix generosity on the part of companies.[27] By making APIs available, website owners invited users to consume their data to mash up with other data, and users accepted the invitation, in turn generating their own new services, improving on the old.[28] Over the past decade, APIs have started to vanish. Some companies have done away with them altogether.[29] Other companies, such as Twitter, continue to offer them, but render them less potent by cutting off users whose usage patterns or purposes suggest

141, §§ 101–106, 132 Stat. 348, 1213–25 (2018). This resulted in the Supreme Court declaring the case moot. United States v. Microsoft Corp., 138 S. Ct. 1186, 1188 (2018) (vacating and remanding judgment).

[25] *See* Josh Constine, *Facebook Is Done Giving Its Precious Social Graph to Competitors*, TECHCRUNCH (Jan. 24, 2013), https://techcrunch.com/2013/01/24/my-precious-social-graph/ [https://perma.cc/43LZ-PJA2].

[26] *See* JOSHUA GANS, ENHANCING COMPETITION WITH DATA AND IDENTITY PORTABILITY 7–8 (2018), https://www.brookings.edu/wp-content/uploads/2018/06/ES_THP_20180611_Gans.pdf [https://perma.cc/5JVU-A7ED] (discussing the value of data to search platforms).

[27] Tim van den Bosch, *The Rise of the Closed APIs*, MEDIUM: DEPT (July 11, 2016), https://blog.deptagency.com/the-rise-of-the-closed-apis-6bd70a353fd5 [https://perma.cc/T3CT-9B4L].

[28] *See id.*

[29] *See id.*

threatening new products that might cut into the platform's business model or growth opportunities.[30]

In contrast, today we see the rise of restrictive APIs, which allow information to be sipped in small doses and subjected to the rules of the data owner.[31] We have seen the rebirth of walled gardens and sterile appliances.[32]

Today, we live in a highly Balkanized online world. This brings me to step three: the benefits of smart Balkanization outweigh the costs. In my remaining two minutes, let me give you four very quick arguments why a Balkanized world, or a world with mild data localization laws, would be a better world for all of us.

Number one: Balkanization rebalances control over local communications, speech, and commerce. By making legible the preexisting borders of our globe, we force Internet providers (and users) to be attentive to border crossings. In the real world, every time I drive into Maryland I see a sign that says, "No texting, no handheld cell phone."[33] (Less helpfully, every time I drive into Texas, a sign says, "Don't mess with Texas."[34] I'm not quite sure what that means.) Data localization rules, if applied wisely, can operate like that.

Number two: my work focuses on the surprising benefits of friction in digital systems.[35] Sometimes friction for friction's sake gives us as a society the opportunity to pause, to communicate, to talk to one another. We're going to discover that friction and inefficiency are often the only paths to incorporating important human values into our digital systems and online spaces.

[30] *See id.*; *see also Twitter Takes on Third-Party Developers with Strict New Rules*, VERGE (June 30, 2012, 1:10 AM), https://www.theverge.com/2012/8/23/3263481/twitter-api-third-party-developers [https://perma.cc/LM85-9QR5].

[31] *See* van den Bosch, *supra* note 27.

[32] *See* JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET: AND HOW TO STOP IT (2008).

[33] Robert Thomson, *Maryland Warns Distracted Drivers*, WASH. POST: DR. GRIDLOCK (Oct. 1, 2010, 11:40 AM), http://voices.washingtonpost.com/dr-gridlock/2010/10/maryland_warns_distracted_driv.html [https://perma.cc/DQ4Q-HQAA].

[34] Alex Mayyasi, *The Surprising Origins of "Don't Mess with Texas,"* PRICEONOMICS (June 11, 2014), https://priceonomics.com/the-surprising-origins-of-dont-mess-with-texas/ [https://perma.cc/983P-CQHS].

[35] *See* Paul Ohm & Jonathan Frankle, *Desirable Inefficiency*, 70 FLA. L. REV. 777 (2018).

Number three: Balkanization hurts the companies a lot more than it hurts you, the individual. In a Balkanized world, companies will have a strong incentive to get to you, so they will find ways to work with countries to surmount the Balkanized structure. Trust me, they will find a way to provide you with your social network, and they're going to find a way to give you access to email. Sure, it might cost them a little bit more money than it does today, but remember, they charge you nothing. At the end of the day, they're the ones who are going to bear the brunt of localization, not you. You are not going to suffer from that change.

Number four: Balkanization might sometimes be better for competition. Some have argued that if all the countries in the world required data localization tomorrow, the only companies that could afford to operate globally would be Google, Facebook, Apple, Amazon, and some of the other giants.[36] I don't think that's true at all. In a world with Balkanization, even those giants would have to make difficult choices about where to enter and where to leave for another day. They would abandon their efforts in some countries—the ones at the bottom of their priority lists.

And what would happen in those localities that have been abandoned by the giants? The vacuum would be filled by local innovation, local innovators, and local technology. This would encourage a wellspring of innovation, shaped with a local flavor, inoculated from competition from abroad, perhaps challenging the monopolization of the foreigners.

Even in the countries that make the cut-off list for the giants, data localization mandates would force the giants to build new data centers in *situ*, meaning they would need to hire local construction workers, deal with local permits, and employ and train local data center employees. All this investment in capital and labor would have spillover effects locally.

My core argument is that our global libertarian fever-dream needs to draw to a close. We should find ways to inject local

[36] *See* Cody Ankeny, *The Costs of Data Localization*, ITI: TECHWONK BLOG (Aug. 17, 2016), http://www.itic.org/news-events/techwonk-blog/the-costs-of-data-localization [https://perma.cc/2ZPY-6S9B] (highlighting impact of localization on "small and medium-sized enterprises").

values, local rules, local respect, and ultimately, respect for local norms and for local society. Thank you very much.

Pierre: So, a rousing defensive Jingoism [Phonetic].

Pierre: You get to vote a second time as well. Jen, over to you.

Jen: Thanks, Pierre. And thanks especially to you, Paul, for (wink) making my job relatively easy.

Paul: Oh.

Jen: I'm going to start with a concession. Borders do matter. As much as John Perry Barlow was a visionary, I'm not suggesting a return to the utopian vision of the world in which governments have no sovereignty in cyberspace.[37] It's not the reality, and it's also not the ideal. Territorial governments do assert control, and they should assert control. After all, the use of the Internet has dramatic cyber-security, national security, and economic consequences. It's where key disputes about speech, and privacy, and other norms are worked out. Governments have a responsibility, and arguably an obligation, to play a role in all of that.

But doing so is messy. Governments across the globe differ in how they view the answers to each and every one of these key governance and normative questions. They differ in terms of how they assess privacy norms. They differ in terms of their assessment as to who should be permitted to access data, according to what substantive and procedural protections, and for what purposes. They differ, as Paul mentioned, in their interpretation of what is, and is not, protected speech. They differ in their assessment of and preferred response to cybersecurity risks. They differ in their views on who should be taxed, how much they should be taxed, and for what activities. And these are just some examples of many.

My thesis is the following: we need to find a way to respect and manage those differences while also promoting to the extent possible, an interconnected Internet that supports the free flow of data across borders.[38] We should and can

[37] *See* Barlow, *supra* note 7; *see also* Michael Schmitt, *In Defense of Sovereignty in Cyberspace*, JUST SECURITY (May 8, 2018), https://www.justsecurity.org/55876/defense-sovereignty-cyberspace/ [https://perma.cc/TQ2S-797X] (discussing the varying approaches regarding sovereignty in cyberspace).

[38] Jennifer Daskal, *Borders and Bits*, 71 VAND. L. REV. 179, 239–40 (2018).

manage differences while also resisting data localization and avoiding Balkanization, particularly at the protocol layer.

And yes, Paul is right. There are many things that are terrible about the Internet. But increased fragmentation and localization is not the answer. There is thus good reason, in my view, that groups like the U.S. Chamber of Commerce and the ACLU, and the EFF all agree on this.[39] They agree because they're right.

[Laughter]

Jen: There also is a good reason why it is countries like China, in enacting its firewall,[40] and Russia, in requiring that all of its citizens' personal data has to be stored locally,[41] are among the most outspoken proponents of localization and the kind of segmented, fragmented Internet that Paul is defending. It is a means of social control. It is a means of keeping tabs on one's citizens. And it is a means of suppressing dissent.

In response to Paul, I will make three arguments in favor of an open, relatively free Internet: economic arguments, rights-based arguments, and security-based arguments. All of these points will be familiar to everyone here, but I will lay out the general claims nonetheless.

Before I do, I want to respond to Paul's descriptive claim about the ways in which technological developments and the decisions of private sector tech companies are themselves fragmenting the Internet. As Paul points out, there is Balkanization at the app level. Data stored on Dropbox is not accessible via iCloud;[42] Twitter and Facebook have self-interested reasons to create barriers between their two

[39] *See* Cooper, *supra* note 17; *Letter from Human Rights Advocates*, *supra* note 18.

[40] *See* Yuxi Wei, *Chinese Data Localization Law: Comprehensive but Ambiguous*, U. WASH. (Feb. 7, 2018), https://jsis.washington.edu/news/chinese-data-localization-law-comprehensive-ambiguous/ [https://perma.cc/N55X-H6U4].

[41] *See* Matthew Newton & Julia Summers, *Russian Data Localization Laws: Enriching "Security" and the Economy*, U. WASH. (Feb. 28, 2018), https://jsis.washington.edu/news/russian-data-localization-enriching-security-economy/ [https://perma.cc/YJ6V-JMYL].

[42] *See Dropbox and MacOS Compatibility*, DROPBOX, https://www.dropbox.com/help/desktop-web/mac-osx-sierra-compatibility [https://perma.cc/4837-4F5E] ("We do not currently support a configuration where both iCloud and Dropbox sync the same files.").

services;[43] and Google seeks to maintain its market dominance via control over information.[44] This is obviously true. But that is a separate problem—grounded in private sector decision making and competition policy—from the issue we are focused on here: government mandated bordering of the Internet as a tool of norm development and control. Consistent with the terms of the debate, my focus is on the latter.

First, the economic benefits. These are well-known. There have been lots and lots of reporting and analysis about the benefits of free trade for the economy.[45] An International Trade Commission report in 2011 concluded that digital trade increased U.S. GDP by approximately four percent.[46] Moreover, the benefits aren't just to the United States. A 2016 McKinsey report says that international data flows increased world GDP by ten percent as compared to a world without such flows.[47]

The ability to access data in big data sets across borders also spurs innovation in ways that are critical to many of the developments that were talked about by panels earlier today. The free flow of data supports innovation in health, in safety, and in educational tools. As one simple example, it is very hard to have an up-to-date, effective language translation product without access to large volumes of foreign language content; this generally requires the movement and accessing data across borders. Tangible benefits in the fields of medicine, health, and safety also result from research involving data sets that move across

[43] *See, e.g.*, Ian Bezek, *Why Facebook Might Need to Buy Twitter Inc*, INVESTORPLACE (Jan. 16, 2018, 12:55 PM), https://investorplace.com/2018/01/why-facebook-might-need-to-buy-twitter/ [https://perma.cc/BG9L-ZAV3] (explaining reasons why Facebook would want to acquire Twitter); Adam Levy, *Facebook's CFO Just Explained Why Twitter and Snap Don't Stand a Chance*, MOTLEY FOOL (May 3, 2018, 9:00 AM), https://www.fool.com/ investing/2018/05/03/facebooks-cfo-just-explained-why-twitter-and-snap.aspx [https://perma.cc/5R2R-F739] (explaining the ongoing competition amongst the two companies); Michael Reilly, *Is Facebook About to Kill Off Twitter?*, MIT TECH. REV. (Jan. 29, 2016), https://www.technologyreview.com/s/546286/is-facebook-about-to-kill-off-twitter/ [https://perma.cc/DDA2-VRD7] (reflecting recent concerns that Twitter's core business would be targeted by Facebook).

[44] *See, e.g.*, *Google Dominates Search. But the Real Problem Is Its Monopoly on Data,* GUARDIAN (Apr. 19, 2015), https://www.theguardian.com/technology/2015/apr/19/google-dominates-search-real-problem-monopoly-data [https://perma.cc/5NKX-HL5M].

[45] *See, e.g.*, DENISE FRONING, THE BENEFITS OF FREE TRADE: A GUIDE FOR POLICYMAKERS (2000).

[46] U.S. INT'L TRADE COMM'N, PUB. NO. 4485, DIGITAL TRADE IN THE U.S. AND GLOBAL ECONOMIES, PART 2, at 13 (2014).

[47] *See* JAMES MANYIKA ET AL., DIGITAL GLOBALIZATION: THE NEW ERA OF GLOBAL FLOWS 10 (2016), http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows [https://perma.cc/UC5TZ9QE].

the borders. This kind of exchange of data is something that should be encouraged.

Conversely, I'm not persuaded by Paul's argument that the closing of borders supports small, local companies—at least not on a significant enough scale to justify data localization mandates and the closing of borders. To be sure, data localization mandates and an array of local, hard-to-meet requirements with respect to data management may result in local companies having a temporary advantage in smaller markets that are not of particular interest to large multinational companies. But in the bigger markets, it is likely to have the opposite effect, ossifying the advantages of the major multinational companies. After all, everybody wants to participate in the bigger economies. But only large companies with sufficiently capacious budgets will be able to effectively manage the different regulations and the different requirements across borders. Small start-ups likely won't be able to compete. The result is the entrenchment of the biggest players and a reduction of meaningful competition on the global scale.

Second, the social and rights-related argument. As I've already noted, local controls are, more often than not, used as a means of stifling dissent, restricting free speech, and asserting various forms of authoritarian control. The examples that Paul used—China, Russia, Bahrain, and Saudi Arabia—highlight this. Requiring data to be stored locally and restricting the free flow of communication puts dissidents and human rights defenders at risk. While those who are the most technologically savvy and the most motivated can and often do find ways to evade some of these restrictions, the overall effect is one of suppression. There is thus a good reason why a free and open Internet has long been a pillar of U.S. foreign policy.[48]

Meanwhile, the oft-claimed rights-based justification in favor of data localization is not supportable. It is not something that Paul mentioned, but in the wake of the Edward Snowden revelations there is a widespread belief that data localization is justified as a means of protecting foreign citizens' and residents' data from excessive U.S. surveillance.[49] This is a red herring for two key reasons.

[48] *See, e.g.*, *Internet Freedom*, U.S. DEP'T STATE, https://www.state.gov/j/drl/internetfreedom/index.htm [https://perma.cc/A26C-N8FZ].

[49] *See, e.g.*, Hill, *supra* note 1, at 29–31.

First, foreign governments' domestic rules governing their own intelligence agencies are often much more permissive and subject to much less oversight than the rules governing U.S. surveillance. As much as U.S. surveillance policies and practices are criticized, they tend to incorporate many more protections and layers of review than the intelligence surveillance practices of foreign governments. Second, the U.S. authority to survey and access data overseas is much greater and subject to much less oversight than the rules that govern the ability of U.S. intelligence agencies to collect data once it's locally held in the United States. Put another way, those worried about U.S. surveillance are often better off if their data is held in the United States than if held overseas, whether pursuant to localization laws or for other reasons.

Pierre: Two minutes.

Jen: And finally, the security costs. One often hears that governments can better protect security by keeping data local. But that too is unconvincing.[50] Cybersecurity is enhanced if caches of data can be kept in multiple locations, protecting it from catastrophic events in any one place. Cybersecurity is also enhanced when companies can choose freely where to host their data, and therefore choose locations that are most secure.[51]

With those arguments as our backdrop, I agree with Paul as a descriptive matter that the trend is one of governments increasingly exerting territorial-based control. But pushing for an increasingly bordered Internet is not the answer. Rather, the goal is to figure out a way to mediate, and manage, those differences, without yielding a fractured Internet. No one should think this is easy. It isn't. But it is something that should be pursued.

Finally, Paul brought up the dispute between the United States and Microsoft about the reach of an American search warrant.[52] I thought I would spend my last minutes using that case to highlight possible ways of managing the

[50] *See* DANIEL CASTRO, THE FALSE PROMISE OF DATA NATIONALISM 1 (2013), http://www2.itif.org/2013-false-promise-data-nationalism.pdf [https://perma.cc/3VQD-JGFZ] ("The notion that data must be stored domestically to ensure that it remains secure and private is false.").

[51] *See* Chander & Lê, supra note 16, at 719–20.

[52] *See* sources cited *supra* note 24.

messiness—and the kind of approach that I think makes sense.

I assume most, if not all, of you know what the dispute is about. But just in case I'll give you the two-minute version. The case dates back to December 2013 when the U.S. government served a warrant on Microsoft asking for emails associated with a particular target in an investigation.[53] Microsoft refused on the grounds that the emails were stored on a server in Dublin.[54] According to Microsoft, this was an impermissible, extra-territorial application of the warrant authority.[55] And it told the U.S. government to go to Ireland and ask the Irish government to help get the data if the U.S. wanted it.[56] The U.S. government fought back.[57] To paraphrase the U.S. government response: that's crazy, you guys move data around all the time, you can access it from within the United States, there's nothing extra-territorial about this at all.[58]

Two lower court judges sided with the government, but the Second Circuit reversed in favor of Microsoft.[59] And the Supreme Court took up the case.[60] The rule according to the Second Circuit was that the location of data determines access.[61] The United States government can, via a warrant based on probable cause, compel production of communications held in the United States. But if the data is held outside of the United States—even if controlled by a U.S.-based company—then the United States government must direct the request to the foreign government where the data is located and wait.[62]

Interestingly, and somewhat ironically, there has been an outpouring of briefs in favor of Microsoft's position, including from a range of groups that support a free and open Internet.[63] But Microsoft's position is that access to

[53] Microsoft Corp. v. United States, 829 F.3d 197, 203 (2d Cir. 2016), *vacated as moot*, 138 S. Ct. 1186 (2018).

[54] *Id.* at 200.

[55] *Id.* at 209.

[56] *Id.*

[57] *Id.*

[58] *Id.*

[59] *Id.* at 222.

[60] Microsoft Corp. v. United States, 829 F.3d 197 (2d Cir. 2016), *cert. granted*, 138 S. Ct. 356 (2017), *vacated as moot*, 138 S. Ct. 1186 (2018).

[61] *Id.* at 222.

[62] *See id.*

[63] *See, e.g.*, Brief of Amici Curiae Elec. Privacy Info. Ctr. (EPIC) et al. in Support of Respondent, United States v. Microsoft Corp., 138 S. Ct. 1186 (2018) (No. 17-2); Brief

data turns on the location of data, which in turn incentivizes the very kind of data localization mandates that all these groups argue against.[64] And, in that regard, Microsoft's position is quite troubling.

On the other hand, there is a legitimate concern that a U.S. government win will be perceived as the U.S. government asserting the authority to access foreigners' data from all over the world simply because they use a U.S.-based company to manage their data.[65] The image is that of an imperialistic United States that fails to respect the kind of borders that Paul says we should respect. And while I disagree with Paul about the solution, I share his perspective that national differences do need to be respected.

But all is not lost. Congress introduced bipartisan-supported legislation just this week that seeks to thread the needle and promote an open, interconnected Internet while also respecting differences across borders.[66] The Clarifying Lawful Overseas Use of Data Act, or CLOUD Act, is sponsored by two Republican and two Democratic senators, and it basically says: yes, the U.S. government should be able to access data without regard to the data location. But if the target of the investigation is a foreign national who is located outside the United States, and if the U.S. request creates a conflict with foreign law, then the U.S. should weigh the relative U.S. and foreign equities in deciding whether or not to enforce the warrant.[67]

It is an attempt to remove incentives for data localization mandates and ensure that access to data does not turn on the happenstance of where the underlying 0s and 1s happen to be located—facts that are often the decision of private

of Privacy Int'l et al. in Support of Respondent, *Microsoft Corp.*, 138 S. Ct. 1186 (No. 17-2); Brief of Amici Curiae of the Reporters Comm. for Freedom of the Press and 40 Media Orgs. Support of Respondent, *Microsoft Corp.*, 138 S. Ct. 1186 (No. 17-2).

[64] Brief for Respondent at 12, *Microsoft Corp.*, 138 S. Ct. 1186 (No. 17-2).

[65] *See, e.g.*, Jennifer Daskal, *Microsoft Ireland Argument Analysis: Data, Territoriality, and the Best Way Forward,* HARV. L. REV.: BLOG (Feb. 28, 2018), https://blog.harvardlawreview.org/microsoft-ireland-argument-analysis-data-territoriality-and-the-best-way-forward/ [https://perma.cc/F273-TZ5T].

[66] S. 2383, 115th Cong. (2018).

[67] *Id.* As discussed *supra* note 24, after we had this debate but prior to publication, the legislation was enacted as part of a larger spending package. *See* Consolidated Appropriations Act, Pub. L. No. 115-141, §§ 101–106, 132 Stat. 348, 1213–25 (2018). For more on this part of the CLOUD Act, see Jennifer Daskal, *Microsoft Ireland, the CLOUD Act, International Lawmaking 2.0*, 71 STAN. L. REV. ONLINE 9 (2018), https://review.law.stanford.edu/wp-content/uploads/sites/3/2018/04/71-Stan.-L.-Rev.-Online-9-Daskal.pdf [https://perma.cc/S3J7-C5HA].

sector actors for things like efficiency and energy costs. At the same time, it seeks to ensure that the interests of foreign governments in protecting their own citizens and their own residents are respected.[68]

I'll just conclude by saying that's the kind of approach that we need. An approach that promotes an open and connected Internet yet also takes steps to reflect and to respect local values. It's messy, it's hard, it's complicated, but it is a worthwhile goal.

Pierre: You know, it's tragic that we have two such superstars and so little time. I wish we had another half an hour, but we don't, so we're going to shorten the cross-examination. We were going to have Jen crossing Paul, and vice-versa, we're just going to have a free-for-all.

[Laughter]

Pierre: We're just going to have a few minutes and each of them can take shots at each other. I'll pile in, so I'll give Jen a second to catch her breath. So Paul, one of the things that struck me is you said, "The Internet is awful."

Paul: Yes, terrible.

Pierre: It's terrible, but it sounds to me, particularly if you listen to what Jen said, the cure that you're proposing is worse than the disease.

Paul: I wasn't a high school or college debater, but I've watched somebody who was in action: Phil Weiser. And one thing I've learned from watching Phil is, every time you begin your part of the debate, you say, "I have three points to make." This is whether or not you have three points to make. You think of the third in the middle of the first. Am I right? Yes, Phil is nodding his head. Yes.

So, I have three points to make. Number one: if we lived in the world from John Perry Barlow's vision, in an online flourishing of a brand-new, organic and emergent democracy like the world has never seen, "the new home of Mind,"[69] then we wouldn't need data localization. But, if you agree with me that the Internet today is terrible, my

[68] S. 2383.
[69] Barlow, *supra* note 7.

solution is the least bad alternative we have. What are our alternatives? Many have been proposed. We can stay with the status quo. We can hope that computer scientists embrace ethics and ethical training. We might turn to multi-stakeholderism,[70] because that has always turned out so well in the past, right? I'm not advocating a rush to a larger role for centralized command and control regulation despite the fact that we have many other appealing alternatives and I just love bureaucracy and totalitarianism. No, we have tried everything else, and everything has failed.

Number two: I do remember when I was studying Oxford-style debate at Hogwarts with Professor McGonagall, I learned that your opponent will often mischaracterize the argument, thereby reframing the terms of the debate. Professor Daskal has mastered this move. In her opening, she mischaracterized my point of view to suggest that I was advocating to close all borders, stick servers in every country on earth and forbid any packets from transiting between any nations. That, of course, is not at all what I'm describing. I think, at the end of the day, she and I are taking positions along a spectrum of the appropriate role for localism.

Number three: Professor Daskal made two claims in the heart of the economic part of her talk, which is that we're going to ossify advantages for giants, and we're going to have trouble disciplining totalitarians. But how has the current borderless Internet been productive at all addressing unchecked corporate power and totalitarianism? Don't we live in a world where giant intermediaries and totalitarians operate at-will and with impunity? If our motivation is to pick the Internet that will restore power to people over corporations and totalitarianism, then clearly it's time to try something new.

Jen: So, let me just start by responding to Paul's vision of doom and gloom. Yes, the Internet is not as open and free and utopian as John Perry Barlow and early Internet enthusiasts imagined. Arguably not even close. But that

[70] Multi-stakeholder approaches provide governance through non-governmental organizations made up of government entities, private companies, civil society members, and other "stakeholders" in a relatively informal, deliberative process. *See* Joe Waz & Phil Weiser, *Internet Governance: The Role of Multistakeholder Organizations*, 10 J. ON TELECOMM. & HIGH TECH. L. 331, 335–40 (2012).

still doesn't mean that increased Balkanization and localized command and control is the answer.

I also fundamentally disagree with Paul that we have tried everything else and everything has failed. To the contrary, we are at an inflection point. We can no longer turn a blind eye to the challenges that have been posed. But there are a number of creative solutions that can and should be attempted, such as the legislative response to the Microsoft Ireland case that I mentioned earlier.[71] The best of these efforts seek to both preserve an open Internet and to respect differences across borders.

The response to the EU's General Data Protection Regulation (GDPR), which is set to go into effect at the end of May 2018, provides an interesting case study.[72] The regulation imposes a wide range of privacy and security-based measures on companies that are offering services in the EU,[73] even if not physically based there.[74] U.S.-based companies, and presumably many others, have for months been engaged in a range of data mapping and privacy assessments in preparation for its implementation.[75] They are doing this because the EU is an important market.[76] Whether or not a company is GDPR compliant is now incorporated into a company's valuation.[77]

Importantly, a range of informal conversations suggests that companies are, in large part, doing so in a holistic way, across their entire systems, and not just seeking to segment the treatment of EU and non-EU data as a means of compliance. This, of course, could change. Companies could ultimately find ways to provide the key protections to EU residents and citizens and not others—thereby providing the kind of segmentation that Paul suggests is (and should be) occurring. But this is not what appears to be currently happening. Instead, the EU is effectively exporting its

[71] *See* sources cited *supra* note 24.

[72] GDPR, *supra* note 22.

[73] *See generally id.*

[74] *See, e.g.*, *id.* at art. 48.

[75] *See, e.g.,* Nina Trentmann, *Companies Worry that Spending on GDPR May Not Be Over,* WALL ST. J. (May 25, 2008), https://www.wsj.com/articles/companies-worry-that-spending-on-gdpr-may-not-be-over-1527236586 [https://perma.cc/5CGC-ECQ8].

[76] *See, e.g.*, *id.*

[77] *See, e.g.,* Memorandum from Davis Polk & Wardwell, L.L.P. on the Impact of the European General Data Protection Regulation on U.S. M&A (Mar. 26, 2018), https://www.davispolk.com/files/2018-03-26_impact_of_the_european_general_data_protection_regulation_on_u.s._manda.pdf [https://perma.cc/T4RG-2SET].

vision of privacy rights and enhanced data security measures across borders.[78]

This may be viewed by some as imperialistic. But it also provides some valuable opportunities—one that could ultimately result in the raising of privacy rights and data security for all. And, to the extent that we increasingly enact borders and celebrate borders, we eliminate those opportunities.

Pierre: You know, one of the things I struggle with, and I guess both of you have a nuanced view of this issue, unfortunately for the purposes of debate. But Jen, when you say, "it's messy," and the goal is to mediate between all these differences, it makes it hard for me to see how you draw lines. Because I've heard this a number of times in the course of the morning, and you actually used the terms yourself: the imperialistic U.S. One of the reasons it seems, to me, why all those parties agreed with everybody except Paul Ohm, is it was in all their interests. They're all U.S. companies.

Paul: Right.

Pierre: So this is actually a form of U.S. cultural imperialism. And I noted the paper tiger and the paper bear and the paper camel that you raised were totalitarian regimes that nobody would agree with, but you didn't address the questions of Brazil, Germany, France, etc. So, those are good national borders, aren't they?

Jen: Brazil is a great example. As Paul mentioned, there was an attempt to mandate a strong data localization law in Brazil.[79] But lots of groups and others opposed it, ultimately killing it.[80] Groups were worried about localization measures being used as tools for domestic repression.[81] Business groups worried about their ability to have

[78] *See CenturyLink is Committed to GDPR Compliance*, CENTURYLINK, https://www.centurylink.com/aboutus/legal/gdpr.html [https://perma.cc/6TZW-GRJJ]; *We Are Committed to Complying with Applicable Data Protection Laws*, GOOGLE, https://privacy.google.com/businesses/compliance/#?modal_active=none [https://perma.cc/YZL7-W25Z]; *Welcome to Twitter's GDPR Hub*, TWITTER, https://gdpr.twitter.com/ en.html [https://perma.cc/4VBF-AGVA].

[79] *See* Chander & Lê, *supra* note 16, at 683–84 (discussing the provision as part of a new draft of the then-proposed Brazilian Civil Rights Framework for the Internet or "Marco Civil da Internet").

[80] *See id.* at 685.

[81] *See* Allison Grande, *Brazil Nixes Data Localization Mandate from Internet Bill*, LAW360 (Mar. 20, 2014, 5:19 PM), https://www.law360.com/articles/520198/brazil-nixes-data-localization-mandate-from-internet-bill [https://perma.cc/MC4G-K3GS].

international access.[82] So, I fundamentally disagree that free and open borders necessarily mean U.S. imperialism. More importantly, lots and lots of smaller countries with smaller markets also recognize that they benefit from an interconnected, relatively open Internet for a range of rights-based, economic, and security reasons.

Pierre: Paul, do you have any questions for Jen?

Paul: We should recognize the pervasive jingoistic chest-thumping at the heart of arguments from those who argue against data localization, the way their chests fill up with pride as they claim, "All the giant online platforms are based in the United States because we have such superior legal and market systems." I'm deeply skeptical of that. I think there is wonderful potential for innovation to flourish in the global south, and among people of color, and among women. Localization mandates are one way we can tap more into those communities. One of the many benefits we'll enjoy from mandating a little more diversity and innovation, is more diverse innovation, which would not be such a bad thing.

Pierre: The question I'd ask you though, and we'll just do two more minutes and each of you take this opportunity to wrap up, and then we'll have a final poll. But, for you Paul, the proposition is: "We need to protect strong national borders." What are those borders to protect us from?

Paul: I am interested in finding space for local, sub-global discussions about human values. Our current system essentially requires us to decide every important question of human values through a straw poll of eight billion human beings. I believe that, and this goes back to Greek theories of democracy, that we're better off trying to ask questions—like, "What do we think about hate speech? What do we think about free speech? What do we think about Nazi memorabilia, revenge porn, or the right to be forgotten?"—among smaller communities. We should debate these value-laden questions first at the city level, at the state level, at the national level, without interlopers from the rest of the world being able to cast a vote just because of the design of technological infrastructure!

[82] *Id.*

Pierre: So, Jen my last question is for you. You mentioned that if we had this Balkanization, we would rather than helping the small companies as Paul said, we'd actually ossify advantages. We'd end up with entrenching dominance. You could argue against that, we already see that. Legaffa (Phonetic), or Fang (Phonetic) is another one. Facebook, Amazon, Netflix (Phonetic), and Google. So, don't we already have dominance, even with the hippy Internet?

Jen: Yes, that was Paul's point. And yes, of course, there are currently a handful of big, major, giant tech companies that have an enormous amount of control. But I don't think the erection of national borders is going to change that. Instead, I fear it will ossify advantage because it is *only* those major companies that have the resources to effectively manage these differences and operate in multiple different jurisdictions simultaneously. The major corporations will effectively price out smaller competitors from this market. So yes, this is an important issue and one that needs to be addressed. But Paul's approach is not the solution.

Separately, on the norms questions and issues associated with speech rights, Paul and I seem to agree that different local jurisdictions should be able to define what is and is not protected speech. But we need to do so in a way that protects, to the extent possible, the open exchange of information. We can, for example, support the use of filtering tools and geolocation technology that generate soft, not hard, borders. This returns me to my refrain: "This is messy, and this is complicated." There is no one-size solution for all of the issues that the Internet presents. But it's a messiness we should embrace.

At the end of the debate, Pierre de Vries polled the audience once again, discovering that some audience members had moved in Professor Ohm's direction:

Poll Statement: "We need to protect strong national borders on the Internet"

Poll Results: Agree – 41.3% Disagree – 58.7%[83]

[83] In the interest of full disclosure, during the administration of the poll, Professor Ohm had threatened the audience that he'd hunt down and discover the identities of those who voted against him.