Statement before the Senate Committee on Commerce, Science and Transportation
Subcommittee on Communications, Technology, Innovation and the Internet
On The Internet and Digital Communications: Examining the Impact of Global Internet Governance

ROSLYN LAYTON, PHD
Visiting Scholar

July 31, 2018

Thank you Chairman Wicker, Ranking Member Schatz, and members the Committee for the opportunity to testify. Chairman Wicker, you are understandably informed of international security and policy issues as chairman of the Helsinki Commission on Security and Cooperation in Europe. Thank you for leadership and commitment to ensure security and defend human rights and freedoms in that role.[1] It reminds me why Mississippi is important to the digital future, just like Manhattan. Mississippi with its population of 3 million has an economy as large as the nation of Ecuador, which has five times the population.[2] Mississippi is innovating in digital technology with telemedicine[3] and precision farming.[4] While we think about digital communications today as search engines, social networks, ecoomerce ,and digital content, as we enter the 5G era, our digital economy will be broadened with smart applications and platforms for health, homes, cities, grids, cars, and infrastructure. We should expect to export these 5G platforms and services. This underscores the importance of today's hearing in getting the policy right. It also demonstrates that every American can benefit and participate in the internet economy and that all Americans have a stake in internet policy.

The economics of the internet allow for the participation of many players. With the evolution to 5G, the next generation mobile standard, and the Internet of Things, this will only increase. Existing businesses will converge, and new ones will emerge. Consider how quickly the US reaped the gains from 4G mobile wireless networks and its associated technologies, apps, and services. Some $100 billion was added annually to the nation's GDP. [5] The windfall from 5G is projected to be even greater: The rollout of a 5G network should is expected to deliver 3 million new jobs and contribute $1.2 trillion to the US economy.[6]

Our country has engaged the question of international technology policy for at least 230 years. Alexander Hamilton's *Report on the Subject of Manufactures* in 1791 advocated for modernizing the American economy to break dependency on slavery and supersede England in manufacturing.[7] We revere Hamilton for his many contributions, which exemplify the importance of a central government. Equally we revere Thomas Jefferson, the exponent of individual freedoms and limited government.[8] As such, the legacy of our policy has been an attempt to balance the necessary role of a central government with the sovereignty of the individual. We maintain that balance through the rule of law and enumerated individual rights. These are values that underpin our approach to international internet governance.

---

[1] Commission on Security and Cooperation in Europe, "Senator Roger F. Wicker," https://www.csce.gov/senator-roger-f-wicker.

[2] Mark J. Perry, "Putting America's Enormous $19.4T Economy into Perspective by Comparing US State GDPs to Entire Countries," May 8, 2018, http://www.aei.org/publication/putting-americas-enormous-19-4t-economy-into-perspective-by-comparing-us-state-gdps-to-entire-countries/.

[3] Morgan Reed, "The Connected Health Initiative Applauds the FCC's New 'Connected Care Pilot Program,'" ConnectedHealth, July 11, 2018, https://www.connectedhi.com/blog/2018/7/11/the-connected-health-initiative-applauds-the-fccs-new-connected-care-pilot-program.

[4] Office of Roger Wicker, "Wicker Leaders New Legislation on Precision Agriculture," press release, January 29, 2018, https://www.wicker.senate.gov/public/index.cfm/weekly-report?ID=60B6C27C-72F6-4147-9F27-A24DA2E5B86A.

[5] CTIA, "How America's 4G Leadership Propelled the U.S. Economy," April 16, 2018, https://www.ctia.org/news/how-americas-4g-leadership-propelled-the-u-s-economy.

[6] CTIA, "Global Race to 5G - Spectrum and Infrastructure Plans and Priorities," April 2018, https://api.ctia.org/wp-content/uploads/2018/04/Analysys-Mason-Global-Race-To-5G_2018.pdf.

[7] Founders Online, "Introductory Note: Report on Manufactures," accessed May 29, 2018, http://founders.archives.gov/documents/Hamilton/01-10-02-0001-0001.

[8] Jules Witcover, *Party of the People: A History of the Democrats*" (Random House, November 4, 2003).

The US tech economy was $1.6 trillion in 2018, 9.2 percent of gross domestic product (GDP). The numbers are even more staggering from an equities perspective; the American tech industry accounts for a quarter of the value of the US stock market, some $34 trillion.[9] There are half a million tech companies in the US with 34,000 new startups in 2017 alone.[10] Globally, the tech industry topped $4.5 trillion in revenue in 2017 and is expected to reach $4.8 trillion in 2018.[11] The US is the single-largest tech market in the world and accounts for 31 percent of the global tech market.[12]

As such, it is in the national interest to shape the international environment by projecting power and securing economic, political, and strategic goods. But the US won't have any credibility if its international internet policy is just about American companies making money. The US must also export a value system that legitimately empowers and rewards other nations to participate in a free-market internet economy, respects the rule of law and individual rights, limits regulatory distortion and abuse, protects property, and delivers measurable improvements in quality of life. This is how we ensure that our regime is most fair, rational, and humane for global internet governance.

Today, I will describe some geopolitical and protectionist efforts proffered by foreign governments as consumer protection, notably the General Data Protection Regulation (GDPR), lax enforcement of intellectual property, and data localization. I will discuss a range of solutions for the committee to consider.

General Data Protection Regulation (GDPR)

In addition to my role at the American Enterprise Institute, I am Visiting Research at the Center for Communication, Media and Information Technologies at Aalborg University in Copenhagen, Denmark. We run a multidisciplinary research and education program looking at the impact of technology in society from engineering, economic, legal, and social perspectives. The GDPR is one of our areas of focus, and I follow it closely.[13]

Europe is the destination for two-thirds of America's digital exports,[14] so naturally we should be concerned when it adopts draconian, misguided regulation. Moreover, the region has fallen precipitously behind on network investment[15] by €150.[16] The 2020 connectivity goals have been pushed out to 2025. Whereas 20 percent of Americans, some 25 million households, have already adopted some kind of pre-5G product or service (e.g. Google Home or Amazon Alexia), Europeans have yet to make this cultural and technological shift.[17] It makes sense that we should broaden and diversify the

[9] Nasdaq, "Technology Companies," _
[10] Cyberstates, "Data Appendix," https://www.cyberstates.org/.
[11] CompTIA, "IT Industry Outlook 2018," https://www.comptia.org/resources/it-industry-trends-analysis.
[12] CompTIA, "IT Industry Outlook 2018."
[13] European Commission, "Data Protection: Rules for the Protection of Personal Data Inside and Outside the EU," http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf.
[14] United States International Trade Council. Digital Trade in the U.S. and Global Economies, Part 1. 2013 http://www.usitc.gov/publications/332/pub4415.pdf
[15]Roslyn Layton, "The EU's Broadband Challenge." American Enterprise Institute. February 19, 2014. http://www.aei.org/publication/the-european-unions-broadband-challenge/
[16]European Investment Bank. "Restoring EU Competitiveness." 2016 http://www.eib.org/attachments/efs/restoring_eu_competitiveness_en.pdf
[17] Strand Consult. "American consumers are already buying 5G products and services while the EU falls further behind on networks and innovation." Spring 2018.http://www.strandreports.com/sw8027.asp

market for our digital goods and services, as EU, if it continued down the current path, will be increasingly incompatible. At the same point, there is not a ready market to replace the EU; China wants indigenous technology. So we need to pursue a strategy that helps the EU and the rest of the world modernize as well as to open China's market. It is becoming increasingly difficult for Brussels to maintain the narrative that its 20-year attempt to regulate its way to growth and competitiveness is working. More Europeans want prosperity than protectionism.

A popular misconception about the GDPR is that it protects privacy; it does not. The GDPR is about data protection or more correctly, data governance.[18] The word "privacy" appears infrequently in the GDPR, only to refer to "Privacy by Design" (Article 25), "Privacy Impact Assessment" (Article 35), the ePrivacy Directive, and the Privacy Shield regime. Data protection is a technical issue whereas data privacy is a legal one.[19]

Harms to consumers, American firms, and competition

Before entering academe, I had a career in digital marketing in Silicon Valley, where I worked with some 2000 American retailers and other online companies. In 2010, I was recruited to the European Union (EU) because of my analytics-based online marketing skills. Meanwhile Brussels began a systematic campaign to dumb down the online experience under the guise of "protecting" consumers. The ePrivacy Directive[20] or so-called "cookie law" launched in 2011, costs EU businesses $2.3 billion annually with no relatable benefit.[21] It is widely recognized as a regulatory failure,[22] detrimental to commerce, and, indeed, counterproductive to privacy and data protection.[23]

The EU continued promulgating punitive regulation without performing regulatory impact analyses of the policies, and ignoring, if not rejecting, the mounting empirical evidence that its approach does not

[18] *What Is the GDPR?*, EVIDON (last visited Aug. 25, 2017), https://www.evidon.com/education-portal/videos/what-is-the-gdpr/.

[19] David Robinson, *Data Privacy vs. Data Protection*, IPSwitch (Jan. 29, 2918), https://blog.ipswitch.com/data-privacy-vs-data-protection.

[20] EUR-Lex, "Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications)," July 31, 2002, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML .

[21] Daniel Castro and Alan McQuinn, "The Economic Cost of the European Union's Cookie Notification Policy," Information Technology and Innovation Foundation, November 6, 2014, https://itif.org/publications/2014/11/06/economic-cost-european-unions-cookie-notification-policy.

[22] Graham Charlton, "The EU 'cookie law': what has it done for us?" Econsultancy. August 27, 2014 https://econsultancy.com/blog/65366-the-eu-cookie-law-what-has-it-done-for-us

[23] W. Gregory Voss, "First the GDPR, Now the Proposed ePrivacy Regulation," *Journal of Internet Law* 21, no. 1 (July 25, 2017): 3–11, https://ssrn.com/abstract=3008765.

fulfill the policy goals it promises.[24][25][26][27][28] Indeed, when implementing the GDPR, the EU ignored the advice of its official research institute on how to create trust in the online environment,[29] notably the importance of consumer education and innovation in privacy-enhancing technologies.[30] After a decade of GDPR-type regulations across EU, consumers report only a marginal increase in trust online. As of 2017 only 22 percent of Europeans shop outside their own country (a paltry increase of 10% in a decade), suggesting that the European Commission's Digital Single Market goals are still elusive.[31] Moreover, only 20 percent of EU companies are highly digitized.[32] These are primarily large firms. Small to medium sized companies invest little to modernize their business and market to other EU countries.

There is extensive evidence that shows that a flexible, innovation-based approach yields software and systems that are better designed to protect data and privacy and that empower enterprises to operate with data protection as a competitive parameter.[33] The International Association of Privacy Professionals' survey of privacy practices of 800 enterprises around the world found that traditionally less regulated industries have more advanced privacy practices than highly regulated industries, which conform only to regulatory requirements.[34] Nevertheless the EU has continued its misguided approach with the GDPR, promulgating 17 invented rights, 35 new responsibilities for bureaucrats, and 45 specific regulations for enterprises.

Following is a snapshot of the American media, retailers, software, and other companies that are no longer accessible in the EU since May 25, when the GDPR went into effect. This is by no means a comprehensive review. Notably people experienced their personal inboxes being flooded with GDPR compliance emails or consent requests attempt to comply with the GDPR, but apparently many of these

---

[24] James Hayes, "'Cookie Law': A Hostage to Fortune?," *Engineering & Technology* 7, no.8 (2012): 66–69.

[25] Elizabeth Aguirre et al., "Unraveling the Personalization Paradox: The Effect of Information Collection and Trust-Building Strategies on Online Advertisement Effectiveness," *Journal of Retailing* 91, no. 1 (2015): 34–49.

[26] Ronald Leenes and Eleni Kosta, "Taming the Cookie Monster with Dutch Law—a Tale of Regulatory Failure," *Computer Law & Security Review* 31, no. 3 (2015): 317–35.

[27] Christina Markou, "Behavioural Advertising and the New 'EU Cookie Law' as a Victim of Business Resistance and a Lack of Official Determination," in *Data Protection on the Move* (Springer Netherlands, 2016), 213–47.

[28] Alan McQuinn and Daniel Castro. "Why Stronger Privacy Regulations Do Not Spur Increased Internet Use." ITIF. July 11, 2018 https://itif.org/publications/2018/07/11/why-stronger-privacy-regulations-do-not-spur-increased-internet-use?mc_cid=6ef5636fad&mc_eid=ff7c0376f1

[29] Layton, Roslyn, How the GDPR Compares to Best Practices for Privacy, Accountability and Trust (March 31, 2017). https://ssrn.com/abstract=2944358

[30] European Union Agency for Network and Information Security. "Privacy, Accountability and Trust- Challenges and Opportunities." February 18, 2011. https://www.enisa.europa.eu/publications/pat-study

[31] European Commission Report. "Use of Internet Services", 2018. http://ec.europa.eu/information_society/newsroom/image/document/2018-20/3_desi_report_use_of_internet_services_18E82700-A071-AF2B-16420BCE813AF9F0_52241.pdf

[32] European Commission Report. "Integration of Digital Technology". 2018. http://ec.europa.eu/information_society/newsroom/image/document/2018-20/4_desi_report_integration_of_digital_technology_B61BEB6B-F21D-9DD7-72F1FAA836E36515_52243.pdf

[33] KENNETH A. BAMBERGER AND DEIRDRE K. MULLIGAN, PRIVACY ON THE GROUND: DRIVING CORPORATE BEHAVIOR IN THE UNITED STATES AND EUROPE (2015).

[34] *IAPP-EY Annual Privacy Governance Report 2015*, IAPP (2015), https://iapp.org/resources/article/iapp-ey-annual-privacy-governance-report-2015-2/.

communications are illegal under the GDPR.[35]

There is no access to Tronc Media, whose flagships newspapers include the *Los Angeles Times*, *Chicago Tribune*, *New York Daily News*, *Hartford Courant* (America's longest running newspaper since 1764), *Orlando Sentinel*, and the *Baltimore Sun*.[36] Access is not available to more than 60 newspapers of Lee Enterprises covering news across 20 states including Illinois, Indiana, Minnesota, Missouri, Montana, Nebraska, Nevada, Washington, and Wisconsin.[37]

Blocked media is not only a problem for the one million Americans who live in the EU and can no longer read news and information about their hometowns, but for Europeans who wish to learn more about the US from direct sources rather than the state-owned media, which dominate the press and broadcasting in most EU countries. To access the internet, Europeans must pay a government media license fee on top of their broadband subscription. The penalty for failing to pay is imprisonment.[38]

It is not just the American media oulets which are down but their advertisers. Given the scope of Google's advertising platform and its affiliates on syndicated networks, its compliance to the GDPR has caused ripple effects in ancillary markets. Independent ad changes noted prices plummeting 20 to 40 percent.[39] Some advertisers report being shut out from exchanges.[40] The GDPR's complex and arcane designations for "controllers" and "processors" can ensnare third party chip makers, component suppliers, and software vendors which have never interfaced with end users, as European courts have ruled that any part of the ecosystem could be liable for data breaches.[41]

Many American retailers, game companies, and service providers no longer sell in the EU. The websites of Williams-Sonoma and Pottery Barn are dark.[42] The online experience of scores of other American retailers is now polluted with pop-ups and disclosures, prompting many customers to click away. Verve, a leading mobile marketing platform with offices in 6 US cities, closed its European operation in advance

---

[35] Alex Hern, *Most GDPR Emails Unnecessary and Some Illegal, Say Experts*, THE GUARDIAN (May 21, 2018), https://www.theguardian.com/technology/2018/may/21/gdpr-emails-mostly-unnecessary-and-in-some-cases-illegal-say-experts.

[36] Alanna Petroff. CNN Money. "LA Times takes down website in Europe as privacy rules bite." May 25, 2018. https://money.cnn.com/2018/05/25/media/gdpr-news-websites-la-times-tronc/index.html

[37] Roslyn Layton (@Roslyn Layton), "Alas, from the EU I can't read @CapTimes and 60 other newspapers across 20 stats in the Lee Enterprises group because of the #GDPR. Freedom and First Amendment R.I.P.," July 26, 2018, 9:47 a.m., https://twitter.com/RoslynLayton/status/1022508758252113920.

[38] Roslyn Layton and Michael Horney, "Innovation, Investment, and Competition in Broadband and the Impact on America's Digital Economy," Mercatus Center, August 12, 2014, 10, https://www.mercatus.org/publication/innovation-investment-and-competition-broadband-and-impact-america-s-digital-economy.

[39] Jessica Davies, *'The Google Data Protection Regulation': GDPR is Strafing Ad Sellers*, DIGIDAY (June 4, 2018), https://digiday.com/media/google-data-protection-regulation-gdpr-strafing-ad-sellers/.

[40] Catherine Armitage. World Federation of Advertisers. July 10, 2018. https://www.wfanet.org/news-centre/life-after-gdpr-what-next-for-the-advertising-industry/

[41] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62016CJ0210&qid=1531145885864&from=EN

[42] Roslyn Layton (@Roslyn Layton), "More #GDPR casualties. @WilliamsSonoma group no longer selling in EU including @potterybarn @PotteryBarnKids @potterybarnteen etc. I can't even access recipes. @caprivacyorg do you really want to shut down this great SF company with your misguided approach?," July 9, 2018, 3:10 a.m., https://twitter.com/RoslynLayton/status/1016248093547945984.

of GDPR, impacting 15 EU employees.[43] Valve, an award-winning video game maker company in Bellevue, Washington, shut down an entire game community rather than invest in GDPR compliance,[44] similalry for Uber Entertainment in nearby Kirkland, WA, which shut down one of its most popular games entirely after a 6 year run because upgrading the platform to GDPR was too expensive.[45] California-based Gravity Interactive no longer offers games in the EU and refunded its European customers.[46] The Las Vegas–based Brent Ozar Unlimited offering a range of information technology and software support services stopped serving the EU.[47] Even the website of the Association of National Advertisers is not available.[48]

If we adopted such a measure in the US, it would likely violate the freedom of speech, as the government requirements are so onerous that they limit expression. As such, we should be weary of California's privacy effort, which bills itself as an American version of the GDPR.[49] Indeed the GDPR's asserted jurisidiction outside the EU may be illegal.[50]

To comply with the GDPR, firms of 500 employees or more will likley have to spend between $1 and $10 million.[51] With over 19,000[52] US firms of this size, total GDPR compliance costs for this group could reach $150 billion, twice the US spend on network investment[53] or one-third of the annual ecommerce revenue in the USA.[54] Hosuk Lee-Makiyama calculates that the GDPR's requirements on cross-border trade flows will increase prices, amounting to a direct welfare loss of €260 per European citizen.[55] The

[43] Ronan Shields. "Verve to focus on US growth as it plans closure of European offices ahead of GDPR." April 18, 2018. https://www.thedrum.com/news/2018/04/18/verve-focus-us-growth-it-plans-closure-european-offices-ahead-gdpr

[44] Steam, "Super Monday Night Combat," https://steamcommunity.com/app/104700/allnews/.

[45] Owen Good. "Super Monday Night Combat will close down, citing EU's new digital privacy law." Polygon. April 28, 2018. https://www.polygon.com/2018/4/28/17295498/super-monday-night-combat-shutting-down-gdpr

[46] Warportal, "Important Notice Regarding European Region Access," http://blog.warpportal.com/?p=10892.

[47] Brent Ozar, "GDPR: Why We Stopped Selling Stuff to Europe," December 18, 2017, https://www.brentozar.com/archive/2017/12/gdpr-stopped-selling-stuff-europe/.

[48] Roslyn Layton (@Roslyn Layton), "Blocked again by #GDPR. Thanks a lot @JanAlbrecht @EU_EDPS. Who needs to use the internet to read blogs and get information anyway? Government censorship parading as privacy and data protection. Sorry @ANAGovRel," June 7, 2018, 4:30 a.m., https://twitter.com/RoslynLayton/status/1004671815426478081.

[49] Roslyn Layton, "Privacy Regulation Insanity: Making the Same Rules and Expecting a Different Outcome," AEIdeas, June 21, 2018, http://www.aei.org/publication/privacy-regulation-insanity-making-the-same-rules-and-expecting-a-different-outcome/.

[50] Kurt Wimmer. Free Expression and Privacy: Can New European Laws Reach U.S. Publishers? Media Institute. November 9, 2017 https://www.mediainstitute.org/2017/11/09/free-expression-and-privacy-can-new-european-laws-reach-u-s-publishers/

[51] PricewaterhouseCoopers, "GDPR Compliance Top Data Protection Priority for 92% of US Organizations in 2017, According to PwC Survey," January 23, 2017, https://www.pwc.com/us/en/press-releases/2017/pwc-gdpr-compliance-press-release.html.

[52] US Census Bureau, "2015 SUSB Annual Data Tables by Establishment Industry," January 2018, https://www.pwc.com/us/en/press-releases/2017/pwc-gdpr-compliance-press-release.html.

[53] Jonathan Spalter, "Broadband CapEx Investment Looking Up in 2017," USTelecom, July 25, 2018, https://www.ustelecom.org/blog/broadband-capex-investment-looking-2017.

[54] US Census Bureau, "Quarterly Retail E-Commerce Sales 1st Quarter 2018," May 17, 2018, https://www.census.gov/retail/mrts/www/data/pdf/ec_current.pdf.

[55] Lee-Makiyama, Hosuk, "The Political Economy of Data: EU Privacy Regulation and the International Redistribution of Its Costs," in *Protection of Information and the Right to Privacy-A New Equilibrium?* (Springer

net effect is that those companies that can afford to will comply; the rest will exit. Hence the GDPR becomes a barrier to market entry, punishing small firms, rewarding the largest players, and enuring regulators into a codependent relationship with the firms they regulate. This is a perverse outcome for a regulation promised to level the playing field on data protection.

Moreover, the GDPR is fundamentally incompatible with Big Data, artificial intelligence, and machine learning with its specific regulation for purpose specification, data minimization, automated decisions and special categories.[56] Some of the most important scientific advances have been the result of processing disparate sets of information in inventive ways, ways that neither subjects nor controllers anticipated, let alone requested. Consider the definitive study on whether the use of mobile phones causes brain cancer.[57] The Danish Cancer Society analyzed the entire population of Denmark born since 1925 by processing social security numbers, mobile phone numbers, and the National Cancer Registry which records every incidence of cancer by social security number. The study is the most comprehensive investigation proving that the use of mobile phones is not correlated with brain cancer.

Security concerns have also emerged. As AEI's internet governance expert Shane Tews declares, "The right to be forgotten is pitted against the right to be informed." [58] A key example is WHOIS, the query and response protocol use to identify those who register domain names is threatened to be masked under the GDPR. Law enforcement, cybersecurity professionals and researchers, and trademark and intellectual property rights holders have a vital interest in the transparency of WHOIS.[59] "The publicly available data that is used to inform threat intelligence networks, find bad actors, and block them from accessing networks will no longer be available under the GDPR," she warns.[60] The situation harkens back to a key fallacy of so-called privacy activists who attempted to block the rollout of caller ID because it violated the privacy rights of intrusive callers.[61] Today we agree that the receivers right to know who is calling is prioritized over the caller.

Global jurisdiction, selective enforcement

In a press conference about the GDPR,[62] Jan Phillip Albrecht,[63] Green Party parliamentarian and "father of the GDPR," assured that GDPR investigations would not focus on small to medium enterprises but

---

International Publishing, 2014), 85–94. This methodology is expanded in Erik Van der Marel et al., "A Methodology to Estimate the Costs of Data Regulations," *International Economics* 146 (2016): 12–39.

[56] Tal Z. Zarsky, "Incompatible: The GDPR in the Age of Big Data," *Seton Hall Law Review* 47, no. 4 (2017): 2.

[57] Use of mobile phones and risk of brain tumours: update of Danish cohort study. BMJ 2011; 343 doi: https://doi.org/10.1136/bmj.d6387 (Published 20 October 2011)

[58] Shane Tews, "Privacy and Europe's data protection law: Problems and implications for the US". AEI.org May 8, 2018. http://www.aei.org/publication/privacy-and-europes-data-protection-law-problems-and-implications-for-the-us/

[59]Shane Tews. "How European data protection law is upending the Domain Name System." American Enterprise Institute. February 26, 2018. https://www.aei.org/publication/how-european-data-protection-law-is-upending-the-domain-name-system/

[60] Supra Tews May 2018

[61] *See* Justin "Gus" Hurwitz and Jamil N. Jaffer, "Modern Privacy Advocacy: An Approach at War with Privacy Itself?, Regulatory Transparency Project of the Federalist Society," June 12, 2018, https://regproject.org/paper/modern-privacy-advocacy-approach-war-privacy/.

[62] European Parliament, Press Conference by Jan Philipp Albrecht, last visited June 24, 2018, https://multimedia.europarl.europa.eu/en/albrecht-general-data-protection-regulation_I155149-A_ra.

[63] Jan Philipp Albrecht, *Auf zu neuen Ufern: Minister für Digitales und Draußen*, (Mar. 3, 2018), https://www.janalbrecht.eu/2018/03/auf-zu-neuen-ufern/ (Albrecht noted that he will not run for reelection in

instead "will concentrate on the bigger ones that pose a threat to many consumers." He noted that firms "already for quite a time now are under suspicion of not complying with European data protection rules" and that they "have been on their screen for years [and] will be the first to be looked at." He indicated that it could be two years before cases are resolved given the process for investigation, adjudication, and appeal. Industry observers suggest that US data brokers (e.g., Axciom, Datalogix, and Equifax) will also be targeted, as well as the auto, pharma, and health care industries.[64]

If smaller companies are trying in good faith to comply with the GDPR, it would be disproportionate to sanction them, Albrecht said, noting that data protection authorities (DPAs) would more likely assist them to become compliant. While the GDPR automatically supersedes national law, only 4 of the 28-member states (Austria, Germany, Slovakia, and Sweden) have completed the formal process to update their local laws to align with the GDPR. If one country rules in a case in its own court, it can be overruled by a majority of the EU nations.

Albrecht argues that enforcement should prioritize the companies that have been on regulators' radar. But if the regulators already know which companies are causing problems, why require every data processor that serves Europeans to comply with preventative regulations? It could be part of a "make-work" strategy to keep Europe's 62 privacy and data protection authorities in business and create jobs for some 75,000 privacy professionals[65] as data protection officers in firms—another GDPR requirement.

Interestingly, Albrecht defends selective enforcement. While the GDPR's stated goal is to make a common standard for every firm, the real goal is to discipline large American firms. This is enabled by the GDPR's enumerated rights of representation, judicial remedy, and compensation, all of which form the basis for regulation by class action. Activists are encouraged to create nonprofit organizations,[66] lodge complaints,[67] and collect damages on behalf of users.[68] Importantly, GDPR complaints cover not just actual injury or harm—which would be required for a class action in US federal court—but failure to comply with regulation, even if no harm results. While class actions can offer consumers a convenient, effective remedy for harm, violation, and noncompliance, they can also be abused by unscrupulous lawyers and activists seeking to bypass democratic policymaking procedures.[69] By legitimizing regulation by class action in the GDPR, the EU creates an incentive for legal abuse. Historically, Europe has largely eschewed "US-style" class actions, noting that they disproportionately reward lawyers over consumers.[70] However, policy entrepreneurs have engineered the GDPR so that privacy activists can bring cases without overcoming legal barriers of standing and jurisdiction—safeguards that help preclude the abuse of the legal system for private gain.

---

the European Parliament in 2018 but take a position as Minister of Digital and Outdoors in the German province of Schleswig-Holstein where he hopes to shape climate and agricultural policy and EU relations).

[64] Laurens Cerulus and Mark Scott, "Who Stands to Lose the Most from Europe's New Privacy Rules," *Politico,* May 23, 2018, https://www.politico.eu/article/the-gdpr-hit-list-who-stands-to-lose-from-europes-new-privacy-rules-facebook-google-data-protection/.

[65] Rita Heimes and Sam Pfeifle, *Study: GDPR's Global Reach to Require at Least 75,000 DPO's Worldwide*, Int'l Assoc. of Privacy Professionals, https://iapp.org/news/a/study-gdprs-global-reach-to-require-at-least-75000-dpos-worldwide/.

[66] "The Right of Data Subjects to Mandate a Not-for-Profit Body, Organisation, or Association," GDPR Recital 142,

[67] "The Right of Data Subjects to Mandate a Not-for-Profit Body, Organisation, or Association," GDPR Recital 141.

[68] "The Right of Data Subjects to Mandate a Not-for-Profit Body, Organisation, or Association," GDPR Recital 143.

[69] Martin H. Redish, *Wholesale Justice: Constitutional Democracy and the Problem of the Modern Class Action,* Northwestern University, 2009.

[70] Redish, *Wholesale* Justice, 32.

Notably Albrecht, European Commission representative Paul Nemitz, and American nonprofit Electronic Privacy Information Center (EPIC) all sit on the board of None of Your Business,[71] a nonprofit founded under the auspices of the GDPR by Austrian privacy activist Max Schrems to bring complaints against American firms. Just seven hours after the GDPR came into effect, it filed complaints against Google and Facebook demanding $8.8 billion in damages.[72]

Schrems' 2013 lawsuit against Facebook single-handedly torpedoed the 15 year old, transatlantic Safe Harbor agreement that processed the data of 4,400 firms, some $250 billion annually.[73] Indeed Schrems' lawsuits are referenced in the brinkmanship of European Parliament, a resolution to end the faithfully negotiated Privacy Shield by September 1, 2018 if the US does not submit to its demands.[74] Many privacy activists are fueled by post-Snowden animus for the US government and could organize a GDPR complaint against a US federal agency with data from European subjects. We already see the automation of complaints—using technology to spam data protection authorities and firms with thousands, if not millions, of complaints at once.[75] Indeed government agencies may be the some of the most vulnerable entities under the GDPR.

In addition to these concerns, there are legal and administrative issues. The GDPR assumes that regulatory authorities have more information than consumers and firms and therefore know better how to order transactions in the marketplace.[76] All the same, the GDPR imposes massive new responsibility on regulators without a concurrent increase in training or funding.[77] EU data supervisors must wear many hats, including "ombudsman, auditor, consultant, educator, policy adviser, negotiator, and enforcer."[78] Furthermore, the GDPR widens the gap between the high expectations for data protection and the low level of skills possessed by data supervisors charged with its implementation.[79] There are certainly many talented individuals among these ranks, but the mastery of information communication technologies varies considerably among these professionals, especially as each nation's data protection authority is constituted differently.

While the GDPR's purported goal is to ensure "fundamental rights," relatively few European users are aware of it. A UK survey found that 34 percent of respondents recognized the law, and even fewer knew

[71] Noyb, "Executive Board," https://noyb.eu/team.
[72] Layton, "Privacy Regulation Insanity."
[73] Roslyn Layton, "Europe's Protectionist Privacy Advocates," *Wall Street Journal,* March 9, 2016, https://www.wsj.com/articles/europes-protectionist-privacy-advocates-1457566423.
[74] European Parliament, "Motion for a Resolution," June 26, 2018, http://www.europarl.europa.eu/sides/getDoc.do?type=MOTION&reference=B8-2018-0305&language=EN.
[75] Privateidentitycontrol.com, "Retrieve the Right to Your Own Identity. Simple and Smooth!," https://www.privateidentitycontrol.com/.
[76] *See generally* F.A. HAYEK, ECONOMICS AND KNOWLEDGE (1937); F.A. HAYEK, THE USE OF KNOWLEDGE IN SOCIETY (1945).
[77] Douglas Busvine, Julia Firoretti, and Mathieu Rosemain, "European Regulators: We're Not Ready for New Privacy Law," Reuters, May 8, 2018, https://www.reuters.com/article/us-europe-privacy-analysis/european-regulators-were-not-ready-for-new-privacy-law-idUSKBN1I915X.
[78] COLIN J. BENNETT AND CHARLES RAAB, THE GOVERNANCE OF PRIVACY: POLICY INSTRUMENTS IN GLOBAL PERSPECTIVE (2006).
[79] Charles D. Raab and Ivan Szekely, *Data Protection Authorities and Information Technology*, COMPUTER L. & SEC. REV. (forthcoming), https://ssrn.com/abstract=2994898.

what it covered.[80] Europeans' dissatisfaction with the EU is well documented.[81] Indeed, voter turnout in European Parliament elections dwindled from 62 percent in 1979 to just 42 percent in 2014.[82] This environment is conducive for the collective action[83] of organized special interests to win over the diffuse majority. Essentially privacy advocates have effectively forced citizens' consent to heavy-handed data regulation in spite of public opinion,[84] which seems to favor a more nuanced approach to privacy and data protection over the sledgehammer of the GDPR.

Conflicting visions of rights and freedoms

Aside from these legal quagmires, the US should not adopt the EU's approach because our notions of privacy come from fundamentally different perspectives. America was founded on the idea that human beings are born with natural rights, such as the rights to life and liberty. These rights are inviolable, God-given, and independent on the laws and customs of the country and, thus, cannot be repealed or restrained by human laws. Natural rights make no demands on others except that they respect those rights. This has been codified in our Constitution and confirmed with over two centuries of case law. Natural rights should be distinguished from human rights, which are moral principles or norms to describe standards of human behavior.

The EU approach, which only came into being in this century, is rather a Johnny-come-lately with the concept of privacy rights bestowed by government and a legal system, and thus can be modified, repealed, and restrained by government. The GDPR, a legal or government-granted right, makes specific demands of others (e.g., demanding how data processors must govern data).

The main authority for privacy enforcement in the US is 15 USC § 45, which charges the Federal Trade Commission (FTC) with preventing "unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce."[85] The FTC took up some 200 cases in 2017 alone.[86] In matters of privacy, the FTC's role is to enforce privacy promises made in the marketplace. Whereas the GDPR assumes that any data collection is suspect, the FTC focuses its enforcement efforts on sensitive information that should be protected against unwarranted disclosure. This helps avoid imposing costly and draconian compliance mandates on entities that are not a priori threats to personal privacy, such as personal blogs, nonprofit organizations, or informational websites. The FTC's approach seeks to allocate scarce regulatory resources to prevent the greatest threats to online privacy. To be sure, if a small entity behaves in an unfair or deceptive way, it can be prosecuted, but the FTC does not assume that every entity wants to harm online users. Additional laws form the foundation on which the

[80] Kirsty Cooke, "Kantar - Data Shows Awareness of GDPR Is Low amongst Consumers," March 27, 2018, https://uk.kantar.com/public-opinion/policy/2018/data-shows-awareness-of-gdpr-is-low-amongst-consumers/.
[81] "Europe's Pressure Points," AEI, January 17, 2017, http://www.aei.org/feature/europes-pressure-points/.
[82] "Turnout 2014 - European Parliament," European Parliament, accessed July 27, 2018, http://www.europarl.europa.eu/elections2014-results/en/turnout.html.
[83] Mancur Olson, *The Logic of Collective Action*. Harvard University Press, January 1971, http://www.hup.harvard.edu/catalog.php?isbn=9780674537514.
[84] Roslyn Layton, "How the GDPR Compares to Best Practices for Privacy, Accountability and Trust," SSRN Scholarly Paper March 31, 2017, https://papers.ssrn.com/abstract=2944358.
[85] 15 USC § 45 (2012).
[86] Federal Trade Commission, "Privacy & Data Security Update: 2017," January 2017–December 2017, https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2017-overview-commissions-enforcement-policy-initiatives-consumer/privacy_and_data_security_update_2017.pdf.

FTC carries out this charge including the Privacy Act of 1974,[87] the Gramm-Leach-Bliley Act,[88] the Fair Credit Reporting Act,[89] and the Children's Online Privacy Protection Act.[90]

The current vogue of normative models for data protection such as the GDPR demonstrate the danger of "privacy overreach," in which the drive to protect privacy becomes absolute, lacks balance with other rights, and unwittingly brings worse outcomes for privacy and data protection.[91] The pace of privacy and data protection law is significantly faster than other laws, leading one scholar to suggest that it threatens to upend the balance with other fundamental rights.[92]

The principle of rational, limited government protects us against the Kafkaesque bureaucratization of regulation in which government agencies enshrine themselves in power in the name of protecting citizens. Totalitarian regimes are built on the premise that power must be increasingly centralized to ensure individual freedom. Every senator on the dais knows what it means to be responsible to the people. Both sides of the aisle and both houses of this Congress care deeply about the issues of privacy and data protection and have attempted to address them in a thoughtful way, respecting the rule of law and individual freedoms, notably Sen. Klobuchar (D-MN) with her bill.[93]

Indeed, there are conflicting visions within the EU itself about which elements of data protection are valuable. A study of Polish university students' monetary valuation of specific GDPR provisions using stated preference discrete choice experiments highlights the enormous gap between research and policy.[94] Researchers estimate that users are willing to pay €6.5/month for a subset of GDPR provisions, notably €1.4/month for erasure and €0.80/month not to be profiled. Interestingly while data portability is valued by policymakers, it was not valued by students. The study also suggests that users could value data protection differently at different points in time and depending on the application used.

If users are willing to pay for specific data protection services, why not allow companies to charge for such services or align their business models based upon their specific consumer preferences? Instead the GPDR increases the cost across the board without meaningfully addressing individual preferences. By requiring all companies to implement such rules, the EU reduces competitive parameters by forcing companies to evolve when the market would otherwise make them obsolete. Informed policy would use randomized controlled trials to find which set of preferences is most valued and efficient. Simply put, the 17 enumerated "rights" represents the wish list of activists, not the evidenced-based request of citizens.

Challenging the GDPR as an Illegal Trade Barrier

We should recognize the GDPR for what it is—a standards war--and make the appropriate response. For

[87] 5 USC § 552a.
[88] 15 USC §§ 6801-6809.
[89] 15 USC § 1681 et seq.
[90] 15 USC §§ 6501-6506.
[91] *Supra Hurwitz*
[92] See Maja Brkan, *The Unstoppable Expansion of the EU Fundamental Right to Data Protection*, *Maastricht Journal of European and Comparative Law* 23, no. 5 (2016): 23, http://journals.sagepub.com/doi/abs/10.1177/1023263X1602300505?journalCode=maaa.
[93] Social Media Privacy Protection and Consumer Rights Act of 2018, https://www.congress.gov/bill/115th-congress/senate-bill/2728/text.
[94] Sabolewski, Maciej and Palinski Michal. How much consumers value on-line privacy? Welfare assessment of new data protection regulation (GDPR). International Telecommunications Society Conference, Passau. July 31, 2017

years Europe has fallen behind in the digital economy. It continues to watch the US, and increasingly China, capture the world market for internet innovation and revenue. So rather than compete on making better internet products and services, the EU competes on regulatory standards. While the EU claims that the GDPR regulates data processing for "mankind," its motives are geopolitical, not humanitarian.[95] While the GDPR's supporters claim its benefit for "everyone", only a select few were involved in its development. Non-Europeans were never consulted on this legislation, nor were they able to vote on its passage. Moreover, the European Parliament didn't consult with global institutions or multistakeholder group before making the GDPR.

The EU made a similar gambit for world dominance in mobile standards by forcing the adoption of 3G/GSM, hoping to trounce the code-division multiple access (CDMA) platform that American operators had invested in. For a time, the strategy gave the European mobile industry (including its six phone manufacturers) a leg up, but the US jumped ahead to 4G and became the world leader in mobile. We should not copy the GDPR but rather leapfrog it with a better approach to data protection.[96]

The EU's GDPR is a form of mercantilism, an economic policy promoting government regulation of the economy to augment state power at the expense of rival nations. It was widely practiced in Europe from the 16-18th century and led to colonial expansion as well as war. Mercantilism is the opposite of the American system, the classic political economy.[97] The GDPR likely violates the World Trade Organization and the Information Technology Agreement and should be challenged as such.[98]

Based on the scientific evidence, the keys to improving trust online are consumer education and incentives for innovation in privacy enhancing technologies. These topics have little to no mention in the GDPR and represent the path for the US to develop a superior approach.

Leapfrogging the GDPR

Consumer Education

While the GDPR claims to empower people, it offers nothing in the way to empower people to educate themselves about how to engage online responsibly. This is likely on purpose because regulatory advocates realize that if people were educated and empowered, they could make their own decisions about how to engage with platforms and would not require government supervision on their online activities.

The GDPR perpetuates a fallacy that making consent more explicit makes consumers more informed. It is like speaking more loudly to a person who speaks another language in the hope that she will better understand. The GDPR requires enterprises to make consent ever more detailed, burdensome and granular without increasing the user's knowledge of the transaction. This creates an increasing chasm between consumer empowerment and bureaucratic control.

Public choice theory also suggests that the EU data supervisors' preferences are not necessarily aligned with the "public interest," what is best for European welfare in the long run. Increasing user knowledge

[95] GDPR Paragraph 4

[96] Roslyn Layton, "Four Ways the US Can Leapfrog the EU on Online Privacy," AEIdeas, May 22, 2018, http://www.aei.org/publication/four-ways-the-us-can-leapfrog-the-eu-on-online-privacy/.

[97] Lars Magnusson, *Mercantilism: The Shaping of an Economic Language*. Routledge, 2015.

[98] Julie A. Hedlund and Robert D. Atkinson. "The Rise of the New Mercantilists: Unfair Trade Practices in the Innovation Economy." ITIF, June 2007. http://www.itif.org/files/ITMercantilism.pdf

and the quality of data protection technology could legitimately make people better off, but it could also render regulators less important. While data supervisors will not necessarily reject policies that improve user knowledge and technology design, it is in their interest to promote inputs that increase their own resources and legitimacy in conducting compliance and adjudication.

As my research details, the EU's official statistics, the Eurobarometer, notes that more than half of all Europeans fail to practice basic privacy-enhancing behaviors.[99] This situation is ripe for improvement and represents a classic example of how consumer education can improve outcomes better, more quickly, and at a lower cost than regulation. Indeed, the first principle of consumer education in data protection, buyer beware, is the first principle for how citizens should protect themselves in cyberthreats in Michael Chertoff's new book on cybersecurity: "Be mindful of what data you transmit and what you connect to your own network."[100] He also recommends practicing cyber hygiene, taking advantage of layered cybersecurity technology, and to outsmart scams with a phone call. Consumers need to practice the same kind of vigilance and personal responsibility in cybersecurity as they do in the data protection domain. Outsourcing the job to bureaucrats will not cut it.

Several private and public organizations have outlined the role of consumer education in online privacy more than a decade ago, but these assets were purposely ignored by the European Parliament in crafting the legislation. Notably, the Organisation for Economic Co-operation and Development (OECD) published a study on Consumer Education for Digital Competence.[101] Key learning points include:

- Linking the concept of digital competence with critical thinking on technology and the media;
- Educating to provide a basis for developing an understanding of the structures and conceptual relationships understanding digital media (e.g., functioning of online market, e-commerce marketing techniques, and user tools);
- Learning the how and why of protecting personal information when using digital media;
- Using media to promote the education of digital competence in compelling ways (e.g., games, videos, blogs, and virtual worlds);
- Age-appropriate education;
- Implementing teacher training; and
- Strengthening multi-stakeholder cooperation to create educational partnerships.

The OECD also published a book to describe prevailing consumer education practices across the member nations, including the institutional frameworks and policy evaluation tools.[102] For example, in the US, the "Teaching Privacy Curriculum" by Serge Egelman et al. offers interactive instruction on 10 principles of online privacy over three weeks in a university setting, a method which has also proved effective to educate and empower users to manage their privacy.[103]

---

[99] *See* Roslyn Layton, *How the GDPR Compares to Best Practices for Privacy, Accountability, and Trust*, at 14 (Mar. 31, 2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2944358.

[100] Michael Chertoff. Exploding Data: Reclaiming Our Cyber Security in the Digital Age. Atlantic Monthly Press, 2018.

[101] Organisation for Economic Co-operation and Development, "Consumer Education Policy Recommendations of the OECD'S Committee on Consumer Policy," 2009, http://www.oecd.org/sti/consumer/44110333.pdf.

[102] Organisation for Economic Co-operation and Development, "Promoting Consumer Education: Trends, Policies and Good Practices - OECD," March 2009, http://www.oecd.org/sti/consumer/promotingconsumereducationtrendspoliciesandgoodpractices.htm#howto.

[103] Serge Egelman et al., "The Teaching Privacy Curriculum," 2016, 591–96.

Innovation in Privacy-Enhancing Technology

The second area with only limited discussion in the GDPR is the role of privacy-enhancing technology. In its report "Privacy Enhancing Technologies: Evolution and State of the Art," the European Union Agency for Network Information and Security (ENISA, now called the Cybersecurity Agency) describes privacy-enhancing technologies (PETs) as "a system of ICT measures protecting informational privacy by eliminating or minimizing personal data thereby preventing unnecessary or unwanted processing of personal data, without the loss of the functionality of the information system."[104] The ENISA report describes a wealth of technologies, but the GDPR only mentions two: encryption/pseudonymisation and data minimization.

ENISA's related report "Privacy and Data Protection by Design" explains privacy enhancing technologies including not only encryption but also protocols for anonymous communications, attribute-based credentials, and private search of databases in addition to a range of strategies of multiple practices that firms can employ.[105] It describes a large body of literature on privacy by design but that its implementation is weak and scattered. Indeed, privacy and data protection features are relatively new issues for engineers, designers, and product developers when implementing the desired functionality. To address this, ENISA has stewarded the discussion on how to develop a repository of such technologies.

Consider how technology and innovation could create better outcomes that prescriptive regulation. The GDPR has extensive reporting, auditing, and compliance requirements, necessitating that enterprises hire data protection officers and that data protection authorities hire workers. These requirements will vastly increase the paperwork created and stored in databases, itself a cybersecurity risk. If the goal is to ensure that entities are practicing data protection, a better system could the audit on demand, or even auditable systems, software which exposes the relevant information to those users who are interested, like ratings used on peer to peer platforms.

It could be that because privacy by design technologies are nascent, policymakers are reluctant to describe them in further detail, though this also contradicts the implicit assumption of the GDPR that data supervisors know best. However, the GDPR-chosen approach of regulation creates path dependency and inevitable outcomes. It clearly puts the thumb on the scale in favor of regulation over innovation.

Such frameworks can have indirect effects in that firms, concerned about inadvertently violating many of the tenets of the regulation and facing steep fines, will choose not to innovate. The GDPR's Article 25 on privacy by design and by default offers little in the way of incentives. There is no safe harbor for data processors to experiment or to implement new privacy by design technologies, so firms risk significant fines if their technologies fail, even if they have an entrepreneurial willingness to employ improved technologies.

[104] European Union Agency for Network and Information Security, "Privacy Enhancing Technologies: Evolution and State of the Art — ENISA," March 9, 2017, https://www.enisa.europa.eu/publications/pets-evolution-and-state-of-the-art.

[105] European Union Agency for Network and Information Security, "Privacy and Data Protection by Design — ENISA," January 12, 2015, https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design.

A review of the literature on the impacts of economic regulation in the information communications technology sector shows a detrimental impact of regulation on innovation.[106] Regulation can create a deadweight loss in the economy as resources are diverted to regulatory compliance and away from welfare-enhancing innovation. A study across all major industries from 1997 to 2010 found that less-regulated industries outperformed overregulated ones in output and productivity and grew 63 percent more. Overregulation increases barriers to entry for entrepreneurs, which slows economic growth.[107] Moreover, regulation can crowd out efforts to create new and better systems.[108]

As early as 2010, the International Conference of Data Protection and Privacy Commissioners resolved that efforts to promote privacy by design needed to be more deeply embedded in policy.[109] The EU could offer grants or rewards for designing better technologies, but those approaches were declined in the regulation. Instead the EU freezes in time one view of data governance to which all controllers must adhere, creating a monolithic attack surface. A better approach is to adopt a policy declaring the importance of data protection and allow entities to evolve the most salient approaches.

The National Institute of Standards and Technology framework offers the most salient way forward to design a 21st-century paradigm of data protection. The focus on the scientific approach ensures the engineering trustworthiness of technology and its incorporation into society. Measurement science and system engineering principles can support the creation of frameworks, risk models, tools, and standards that protect privacy and civil liberties.[110] As such, Americans can develop a better regime through science, technology, and innovation. Policymakers can incentivize this with partnerships for grants, prizes, award, competitions, and safe harbors for innovation to ensure that innovators can innovate without punishment.

Data Localization

Related to the protectionist GDPR is data localization. Increasingly, countries are forcing firms to store data locally, inhibiting the free flow of information and creating a Balkanized internet. Some 34 countries have enacted barriers[111] to restrict data—whether financial, personal, government,

[106] Luke Stewart, "The Impact of Regulation on Innovation in the United States: A Cross," Information Technology and Innovation Foundation, June 2010, 18, http://www.itif.org/files/2011-impact-regulation-innovation.pdf.
[107] Antony Davies, "Regulation and Productivity," Mercatus Center, May 7, 2014, https://www.mercatus.org/publication/regulation-and-productivity.
[108] Patrick McLaughlin and Richard Williams, "The Consequences of Regulatory Accumulation and a Proposed Solution | Mercatus," Mercatus Center, February 11, 2014, http://mercatus.org/publication/consequences-regulatory-accumulation-and-proposed-solution.
[109] European Data Protection Supervisor, "International Conference of Data Protection and Privacy Commissioners," October 27, 2010, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Cooperation/Conference_int/10-10-27_Jerusalem_Resolutionon_PrivacybyDesign_EN.pdf.
[110] Paul Hernandez, "Cybersecurity and Privacy Applications," National Institute of Standards and Technology, August 23, 2016, https://www.nist.gov/itl/applied-cybersecurity/cybersecurity-and-privacy-applications.
[111] Nigel Cory, "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?," Information Technology and Innovation Foundation, May 1, 2017, https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost.

telecommunications, or others against digital services. The United States International Trade Commission describes the importance of global digital trade and the many barriers.[112]

Countries claim that they need data localization to ensure data privacy and cybersecurity, help the local digital economy, and ensure government access to data, but these reasons are unfounded. Cyber threats transcend borders, and the data's location is not a deterrent to criminals. While firms take advantage of multiple locations for data centers, these centers offer limited support to economic growth. The proper strategy to support the local digital economy is to focus human capital to create digital goods and services in the country itself. Governments can get access to data when they need to with the appropriate court orders; the length of time of delivery is a matter of seconds.

Data localism should be addressed appropriately by the rule of law, at the World Trade Organization, and with other appropriate institutions.

Intellectual Property

Just as we can describe Title II internet regulations as government taking the physical property of networks, the GDPR is government taking the intellectual property of algorithms. Both regulations deny their owners their rights of ownership and innovation.[113]

Protection of intellectual property is enshrined in our Constitution.[114] James Madison reiterated the Copyright Clause in Federalist Paper No. 43 noting, ''The utility of this power will scarcely be questioned. The copyright of authors has been solemnly adjudged, in Great Britain, to be a right of common law. The right to useful inventions seems with equal reason to belong to the inventors."[115] The product that a person creates with his hands is no different than what he creates with his voice or brain. The creator has the right to decide how to monetize his creations.

As of December 2016, copyrighted works contributed an estimated $1.2 trillion to the US GDP,[116] accounting for 6.88 percent of the US economy, almost as large as the $1.6 trillion internet economy itself.[117] The internet intermediaries enjoy intellectual property (IP) protection for their software and algorithms. It is illogical that the software property protections are honored internationally but not the content they deliver. The US loses about $300 billion annually from the theft of copyrighted materials.[118]

Fortunately, advances such as machine learning and cloud computing enable online intermediaries to accurately and efficiently identify known-infringing content, particularly content that rightsholders have

[112] United States International Trade Commission, "Despite Huge Growth in Global Digital Trade in Recent Years, Some Countries Seek to Slow Adoption, Reports USITC," press release, September 28, 2017, https://www.usitc.gov/press_room/news_release/2017/er0928ll836.htm.
[113] Roslyn Layton and Bronwyn Howell, "How Title II Harms Consumers and Innovators," American Enterprise Institute, July 14, 2017, http://www.aei.org/publication/how-title-ii-harms-consumers-and-innovators/.
[114] The Constitution of the United States (Article I, Section 8, Clause 8) grants to Congress the powers to promote "the progress of science and useful arts" by providing inventors the limited but exclusive right to their discoveries. This applies to copyrights and patents, with trademarks similarly protected by Congress under the Commerce Clause (Article I, Section 8, Clause 3). Together, they are all protected under the umbrella of intellectual property.
[115] James Madison. Federalist No. 43. January 23, 1788
[116] Stephen E. Siwek, "Copyright Industries in the US Economy," International Intellectual Property Alliance, 2016, https://iipa.org/files/uploads/2018/01/2016CpyrtRptFull-1.pdf.
[117] Comp TIA, "Cyberstates," https://www.cyberstates.org/. 2018
[118] Supra Siwek.

shown belongs to them. Technologies and business models continue to improve making detection of pirated, unlicensed content more efficient, meaning that we can have a strong copyright standard without overburdening intermediaries. For example, ad networks can restrict the use of advertising on sites with known infringing content, which helps restrict revenue to those criminal enterprises designed to illegally exploit copyright-protected content. Such tools combat not only pirated content but also harmful and pirated goods such as counterfeit medicines.[119]

Like the network regulation debate, the copyright-free movement is a coalition of some large tech companies aligned with anti-IP groups that want to restrict if not abolish copyright protections.[120] Some copyright "minimalists" argue that since they would not have paid for the products, stealing improves consumer welfare. Others see piracy as merely a form of societal redistribution from rights owners to consumers. They leverage databases of millions of users to overwhelm political process and create the appearance of grassroots support, for example one million signatures on a Change.org petition. This is not an authentic reflection of the people but rather the amplified support of the digital elite.[121] Some countries recognize that they do not produce a significant amount of exportable digital content, so they see no strong incentive to have strong digital copyright enforcement. Instead, they see opportunities to create digital platforms that leverage the content produced by others, particularly US creators.

Another hypocrisy has emerged in that many advocates of the copyright-free moment want regulation to ensure their unfettered access to content regardless of the copyright concerns but see no problem when the onerous GDPR requirements force content owners to stop serving the EU. Similarly, they celebrate the liability protections of the Communications Decency Act[122] and the Online Copyright Infringement Liability Limitation Act[123] afforded to highly regulated common carriers in telecommunications, but don't see that the same common carriage should apply to their preferred internet platforms which are also granted immunity under the Acts. Such legal policy inconsistencies should be investigated and resolved.

Ideally, by creating transparency to the competing interests, the debate can move forward on the merits of the arguments. In any case, without copyright, the individual creator has no protection for his work, so supporting this position is vital to ensure individual rights.

Some reasons for the decline in US internet leadership

The US had a leadership role in internet governance, but lost it. When the US fails to uphold the rule of law in its own country, it gives license to other nations to do the same. Moreover, the US failed to

[119] Daniel Castro, "PIPA/SOPA: Responding to Critics and Finding a Path Forward," Information Technology and Innovation Foundation, December 5, 2011, https://itif.org/publications/2011/12/05/pipasopa-responding-critics-and-finding-path-forward.
[120] Richard Bennett, "Europe's Piracy Dilemma, High Tech Forum, July 5, 2018, http://hightechforum.org/europes-piracy-dilemma/.
[121] Roslyn Layton, "Net Neutrality: A Numbers Game," AEIdeas, July 25, 2016, http://www.aei.org/publication/net-neutrality-numbers-game/; Change.org, "Stop the Censorship-Machinery! Save the Internet!," https://www.change.org/p/european-parliament-stop-the-censorship-machinery-save-the-internet; and Roslyn Layton, "Dominated by the Digital Elite," *US News & World Report*, August 8, 2017, https://www.usnews.com/opinion/economic-intelligence/articles/2017-08-08/the-digital-elite-dominates-debates-over-net-neutrality-and-title-ii-rules.
[122] 47 USC 230
[123] 17 USC 512

challenge those countries that violate digital trade agreements. During this period in which the US has slackened in it own practice of the rule of law, there has been a shift of the international view of America over the past 20 years from one of respect and reverence to one of resentment. The Pew Research Center's Global Attitudes and Trends reports that other nations' opinions of the US have diminished from preeminence to a tie with China for the world's most popular nation.[124]

To a number of foreign nations, the explosion of free speech restrictions on American college campuses legitimize the efforts to clamp down on journalists, dissidents, and other critics of government. In the internet space, a recent and egregious example was in 2014–15. The Federal Communications Commission pronounced that one of its greatest inventions—the internet—is a mere extension of the telephone network and thus a utility to be regulated by the government. It was a slap in the face to engineers and inventors whose life's work was creating an alternative to the telephone. It disrespected their inventions and the technologies of freedom. In addition, it trampled the rule of law, in which the people certified through Congress that the internet is to be free and unfettered from state and federal regulation. The move to declare the internet a utility was welcomed by many unsavory nations as perfect justification to apply their favorite form of government control on the internet. It is no surprise that dozens of nations have engaged in harmful regulation toward the US, a country they once respected. Moreover, internet freedom has been declining for the past seven years despite increasing regulation around the world purported to protect consumers and "openness."[125]

This abuse is not limited to government. Leading Silicon Valley firms have waged a campaign to impose internet regulation on the telecom industry to avoid interconnection fees and preclude the development of competitive business models for content and advertising.[126] While it may be a rational strategy for Silicon Valley, it is wrong and unfair to employ political means to secure price controls that undermine the efficient functioning of internet markets. As I have demonstrated with more than 5 years of doctoral and post-doctoral research, these regulatory policies have been harmful in the US and abroad, concentrating internet traffic to fewer players and enshrining a monoculture of platform paradigms and business models.[127]

The imposition of price controls denies infrastructure providers revenue to build networks (and tax revenue for governments), undermines the emergence of business models that could support local content development for socially beneficial goods (particularly in developing countries), and unduly burden consumers with the full cost of networks, a cost that falls disproportionately on the poor. Moreover, the politicized regulatory exercise distracts scarce policymaking resources away from real problems, which are empirically demonstrated to be the malign acts of governments to censor people,

---

[124] Global Indicators Database, "Do You Have a Favorable or Unfavorable View of the U.S.?," Pew Research Center, http://www.pewglobal.org/database/indicator/1/.

[125] Roslyn Layton, "The Link Between Net Neutrality and Declining Internet Freedom," AEIdeas, December 15, 2015, http://www.aei.org/publication/link-net-neutrality-declining-internet-freedom/. For an updated report, see Freedom House, "Manipulating Social Media to Undermine Democracy," https://freedomhouse.org/report/freedom-net/freedom-net-2017.

[126] Internet Association, "Net Neutrality," accessed July 19, 2018, https://internetassociation.org/positions/net-neutrality/.

[127] Roslyn Layton. *Which Open Internet Framework is Best for Mobile App innovation? An empirical inquiry of net neutrality rules around the world*. Aalborg University, 2017. http://vbn.aau.dk/en/publications/which-open-internet-framework-is-best-for-mobile-app-innovation(b1f05c8d-b31e-47cd-b19d-bcf6893e7e5b).html

services, and data.[128] Indeed, many internet-related firms and industries have taken advantage of the regulatory process to win favorable treatment for themselves at the expense of their competitors and consumers. Foreign counterparts have learned from the rent-seeking behavior of Americans firms, and it has boomeranged. Now foreign governments find ways to regulate American firms to reward their domestic players.[129]

Moreover the US has distracted itself with phantom fears and instead of focusing on real threats. The US may have been the leader in 4G, but leadership is not assured in future generations. The Chinese government wants its country's device, app, and service developers to win the race for the 5G ecosystem. China has already replaced the US as the world's largest mobile app market,[130] unseating the US in downloads and revenue in 2016. The US, caught up in crony squabbles and rent-seeking regulation over the past decade, took its eye off the ball. The real threat to Silicon Valley is not the nation's 4,551 internet service providers, but rather Chinese internet giants, including Baidu, Alibaba, and Tencent, which make the US players look tame by comparison.[131]

Unless it wants to capitulate for China, American industry needs to set aside its crony games and start to play for Team USA. Telecom, content, software, and hardware companies should all play for the same team. They should partner to complement each other's strengths, leveraging the appropriate actors for the conversation. Moreover, Team USA should grow the bench and bring new valuable actors into the fold. The more robust our market and diversified our business models, the less likely China will be able disrupt it.[132]

Earning the leadership role again

The US needs to model the behavior it wants to see in the world by upholding the rule of law and respect for individual rights. When American enterprises operate abroad—whether they are for-profit corporations or nonprofit entities—they want a rational, predictable, and consistent framework across the board. Such a framework allows the enterprise to minimize costs, maximize revenue, ensure efficiency, and allow improvement and innovation. To ensure the ideal framework *abroad*, enterprises should advocate for the ideal framework at *home*. Therefore, the policy should be a consistent set of rules for all players, grounded in modern, evidenced-based standards of antitrust and delivered by the FTC.[133] This also requires removing the asymmetric regulation and regulatory prejudice that have stymied innovation in business models and platforms.

We must also let go of antique notions of internet architecture and outdated regulations that prohibit

[128] Freedom House, "Freedom on the Net 2017," https://freedomhouse.org/report/freedom-net/freedom-net-2017.
[129] Roslyn Layton, "Net Neutrality Will Be Reincarnated as Platform Regulation," AEIdeas, December 20, 2017, http://www.aei.org/publication/net-neutrality-will-be-reincarnated-as-platform-regulation/.
[130] App Annie Content, "App Annie Mobile App Forecast: China to Surpass the US in 2016," accessed July 19, 2018, https://www.appannie.com/en/insights/market-data/mobile-app-forecast-china-to-surpass-us-in-2016/.
[131] CTIA, "How America's 4G Leadership Propelled the U.S. Economy"; Raymond Zhong, "Worried About Big Tech? Chinese Giants Make America's Look Tame," *New York Times*, May 31, 2018, https://www.nytimes.com/2018/05/31/technology/china-tencent-alibaba.html.
[132] Sara Fischer, "U.S. Big Tech Is Still Beating out China," Axios, July 24, 2018, https://www.axios.com/us-big-tech-china-silicon-valley-fe76b105-d9d0-4b34-8632-7e91b8f6d9a2.html.
[133] Richard Bennett et al., *Comments on Communications Act Modernization*, January 31, 2014, https://ssrn.com/abstract=2388723.

innovation e.g., this wooden notion of network core and edge. It is precisely these regulatory prejudices that have precluded the network design advancements that can improve security.[134] It was a reasonable to trust the digital community in the days of the ARPANET when the users were a handful of scientists and engineers. With billions of internet users today, assumed trust is not an option. Cyberattacks and threats are commonplace and demand to be addressed within the framework of defense. Perpetrators of cyberattacks, notably rogue states, should be punished by ending visas, freezing assets, and other punitive tools of international law. Modern cybersecurity requires advanced information-sharing among global partners, a market for cyber insurance, freedom of parties to exercise self-defense, and the augmentation government's coordination with military, business, and hacker communities.[135] Some suggest that the cybersecurity crisis is the outcome of obsolete networked computer architecture and demands a new paradigm of cryptography, the architecture of blockchain, and its derivatives. It is suggested that this emergent architecture will enable a new form of payments on the internet and topple reigning monopolies.[136]

Let me close with a story that demonstrates how the US pursuing its national interest has been a force for good.[137] Upon coming into office, Thomas Jefferson was confronted of the problem of American merchant ships being seized by the Barbary States of Northern Africa; the goods were confiscated and the crews enslaved. Most countries paid ransom so that they could traverse the Mediterranean. American representatives had tried negotiation for some 20 years, but the situation grew worse. Over 1 million Europeans and Americans had been captured by the Barbary pirates over the period.

On the eve of his inauguration, Jefferson's request to Congress was authorized, dispatching naval ships to the region to recover the hostages and destroy the pirate fleets. Sweden and Sicily joined the effort because they too had suffered the Barbary scourge. After a series of battles, the US emerged victorious, returned the stolen goods to the various European nations, and returned to the US with the American hostages. The Barbary Wars became a vindication for Jefferson whose critics wanted him to focus inward on the Louisiana purchase. Winning the Barbary Wars solidified free trade in the Mediterranean.

Just as Jefferson had to secure the sea lanes for trade in the 19th century, we must secure the information lanes for the free flow of data in the 21st. Otherwise we appease mercantilist nations by letting them violate international law, and the situation grows worse. Ideally the issues can be resolved in the context of trade negotiation. Alternatively, we can create a better regime which becomes so popular that the rest of the world joins it, isolating the mercantilists. Or we can fight. This is not to suggest a military war, but a war in the court.

---

[134] Jaikumar Vijayan, "Net Neutrality Could Hinder Efforts to Safeguard Web, Worry Security Experts," *Christian Science Monitor*, February 27, 2015, https://www.csmonitor.com/World/Passcode/2015/0227/Net-neutrality-could-hinder-efforts-to-safeguard-Web-worry-security-experts.

[135] Jeffrey A. Eisenach et al., "An American Strategy for Cyberspace: Advancing Freedom, Security, and Prosperity," American Enterprise Institute, June 3, 2016, http://www.aei.org/spotlight/american-strategy-for-cyberspace/.

[136] George Gilder, *Life After Google: The Fall of Big Data and the Rise of the Blockchain Economy* (Gateway Publishers, 2018).

[137] Gordon Wood. *Revolutionary Characters: What Made the Founders Different*. Penguin Press, 2006.