Promoting Economic Prosperity in Cyberspace

Daniel J. Weitzner

The Internet's inherent flexibility, its carefully constructed public policy foundations, and the universality of its technical underpinnings as an open platform have given rise to extraordinary economic growth around the world. As such, the economic flourishing of the Internet, and the society around it, depends on keeping the Internet ever-evolving as a work in progress. This is ever more urgent as the social, political, and technical conditions that applied at the Internet's inception have come under serious pressure in recent years. The greatest current challenges include the vast collections of personal data and breathtaking analytical tools that put personal privacy at risk; the technical power and increasing dominance of the major Internet platforms; and the rise of technically sophisticated authoritarian regimes.

This essay assumes that the "prime directive" for Internet policy going forward should be to promote economic prosperity. While other social and political imperatives are equally important, it bears reflecting on whether the virtuous cycle of growth that has generated economic benefits along with substantial public good in the first phase of the Internet's development can be continued into the future. The economic success of the Internet, while not evenly distributed, has reached into every region of the world and nearly all aspects of human life. In the United States alone, recent estimates indicate that the Internet sector accounts for roughly 6 percent of GDP.[1] This measure of value, however, represents just the tip of the Internet iceberg as a multitude of businesses all over the world are built on the services offered by cloud computing offerings, such as Amazon EC2 and Microsoft Azure. Indeed, operating systems offered as platforms form the basis of industries far beyond just the information technology sector. Still, advancing the long-term and sustainable economic success of the Internet should

Ethics & International Affairs, 32, no. 4 (2018), pp. 425–439.

doi:10.1017/S0892679418000606

not, and cannot, be separated from consideration of broader social and political concerns.

In considering the ideal ingredients for economic success, the first section of this essay considers the essential technical and legal foundations that gave rise to the Internet's current dynamism. Moving from there, the second section discusses new challenges that have appeared along with the maturation of the Internet environment, offering some ideas about how to ensure that the Internet remains an economic growth engine in the face of these challenges. While some of the original foundations of the Internet are in need of modification, ensuring a cyberspace that promotes economic prosperity as the highest priority would largely entail taking seriously the basics that brought us this far.

The Foundations of Internet Policy

The development of the early commercial Internet was enabled by a particular set of legal and policy foundations. Most were first put into place in the United States in the mid-1990s and over the next decade took root in similar form in advanced industrialized countries around the world. I have identified six foundational elements of early Internet policymaking that were essential to its economic success:

1. Freedom of expression and user empowerment
2. Liability limitation and responsibilities
3. Rights-based regulation of government surveillance
4. Open technical and operating standards
5. Privacy protection
6. Net neutrality

Another set of enabling elements for the Internet's economic success are the policies and programs associated with technology research and development that have been supported by governments in Asia, Europe, and North America. These programs have their own set of normative principles and priorities that will not be explored here, but it is important to note that without them many of the core technologies that make up the Internet would have been simply unavailable.

Freedom of Expression

From its earliest design, the Internet's core mission has been to promote the free flow of information, so there has been an essential connection between the

operation of the Internet and legal protections for the right of freedom of expression.[2] Due to the early adoption of Internet infrastructure in the United States, the first interactions between the U.S. legal system and the Internet had an outsized impact on the way policymakers around the globe approached Internet policy questions. In granting strong free speech protections to all who used the Internet, the U.S. Supreme Court took a step that was a boon to democracy and that paved the way for a vibrant marketplace of information-based goods and services.[3] There were still some narrow categories of speech that were not protected: child pornography in most countries, hate speech in many places, and xenophobic/nationalistic/anti-Semitic speech in several European countries. But in the main, protection of the fundamental right of free expression stood as an early foundation of Internet law where the technology developed most aggressively.

Liability Limitation and Responsibilities

A unique aspect of the industrial organization of the Internet economy is its dependence on platforms, that is, Internet intermediaries such as Google, Amazon, YouTube, Facebook, Twitter, Microsoft Azure, and eBay, joined in recent years by Alibaba, Tencent, Baidu, and others. These platforms offer essential services, such as search, social networking, file hosting, video distribution, cloud computer services, and commerce platforms. Platforms are vital to the Internet economy for two reasons. First, platforms such as Amazon cloud services, Google Apps, Microsoft Azure, and Alibaba cloud have become indispensable foundations for a wide variety of established business enterprises and start-ups. Much of the broad impact of the digital economy across all sectors depends on the ubiquitous and affordable access to cloud services provided by these platforms. Second, the U.S. platforms themselves are huge revenue generators, with the GAFAM (Google, Apple, Facebook, Amazon, and Microsoft) commanding a combined market capitalization of more than $4 trillion.

Thus, the viability of Internet platforms depends on a critical second foundation of Internet policy: liability limitation and legally defined obligations set out for information intermediaries. Early Internet platforms were able to grow because they had only limited liability for harm caused by their users. For example, if a YouTube video or a social media post caused legal harm, the user, not the platform, was (and still is) considered legally responsible. Proscribing limitations on legal liability for platforms as part of the Communications Decency Act of 1996

was the first affirmative step that the U.S. government took in regulating the Internet, aside from an unsuccessful censorship law.[4] The European Union soon adopted similar rules, and the Organisation for Economic Co-operation and Development (OECD) recognized the economic necessity of intermediary liability limitation in its 2011 *Recommendation of the OECD Council on Principles for Internet Policy Making*.[5] Taken together, these rules allowed Internet platforms to grow quickly and expand around the world, offering low-cost or free services because they were largely free from the risk and expense of potential liability from their users' activities. This liability limitation has never meant that responsibility for online harm was legally eliminated, but rather that those who alleged harm had to seek recompense from the users directly, as opposed to the platforms through which the harm was perpetrated.

Policymakers sought to limit platform liability for third-party content to incentivize platforms to police content on their own systems. The U.S. Congress believed that platforms were in a better position than state censors to create environments that would be seen as trustworthy and safe by their users.[6] Platforms at the time were reluctant to remove even objectionable content from their services for fear of being held legally liable, as if they were the editor of all third-party content on their sites. So, legislatures in the United States, Europe, and elsewhere provided liability protections in order to encourage them to take steps to remove harmful content.[7] There was also an understanding that the technological state of the art at the time was such that automatic prescreening of content was impractical. Therefore, if platforms were held responsible for third-party content, and were to respond effectively to preempt the cost of violation, they would likely have to limit speech opportunities for their users substantially because of their inability to screen content before posting.

Rights-Based Regulation of Government Surveillance

As digital communications technologies grew, law and policy came under pressure to provide concomitant protections for users against unjustified government surveillance of these platforms. The U.S. Congress passed the Electronic Communications Privacy Act in 1986,[8] which accorded email the same protection as first-class letters against both government and private surveillance. Much more broadly, the European Convention on Human Rights protects citizens against government surveillance except in circumstances where such surveillance is necessary and proportionate to the crime being investigated.[9]

https://doi.org/10.1017/S0892679418000606 Published online by Cambridge University Press

Another important aspect of the privacy debate was the struggle over access to encryption technology—the technology that allows for the protection, confidentiality, and integrity of digital data and communications. Until the late 1990s cryptography had been controlled as a munition by many countries, including the United States. However, in order for a public Internet to function as a user-friendly and economically robust environment that could protect financial, health, and other personal data, there was clearly a need to deregulate the use of encryption and to enable security to be embedded into the Internet infrastructure. Hence, the United States government liberalized long-standing export control rules as applied to mass market software and hardware. Today, access to strong encryption and secure systems is an economic nonnegotiable. Not only do businesses and individuals need to know that their data is generally secure, the Snowden disclosures raised genuine technical and marketplace concerns about the risk of unauthorized intrusion by intelligence agencies. Nonetheless, law enforcement and national security agencies have lobbied to build so-called back doors or exceptional access into encryption systems to enable government surveillance of data even if the user protects it with strong encryption. This debate is ongoing, though there is a general recognition that back doors in security systems create infrastructure-wide risks for all users, not just for those who are legitimate surveillance targets.[10]

Open Technical and Operating Standards

Today's global Internet is quintessentially a public infrastructure, relied upon by billions of people and properly the subject of interest by governments. Yet the origin story of the Internet is quite different from other media. Since their earliest days, communications media such as broadcast radio, television, and cable television have relied on the indulgence and permission of governments for things such as radio spectrum licenses and rights of way over public lands. The Internet and the World Wide Web developed through ad hoc, global, and decidedly nontreaty-based technical organizations, such as the Internet Engineering Task Force (networking technical standards), the World Wide Web Consortium (web technical standards), and ICANN (administrative rules for Internet domain names).[11]

The engineers who came together to design the Internet and the Web were able to work quickly to lay the technical foundations for this rapidly growing global infrastructure. And in many cases, upstart innovators gained advantages in the nascent Internet marketplace over established telecommunications incumbents because of the rapid pace of innovation. If government had been more involved

from the outset, issues such as security, privacy, and equitable access might have been given more priority. Instead, the open environment allowed for largely unfettered economic growth.

The role of these nongovernmental, ad hoc, global standards bodies is not without controversy, however. Following the urging of Russia, China, and other authoritarian regimes, the United Nations has periodically tried to assert control over key aspects of the Internet technology and operating agreements. Those efforts have been rebuffed, generally at the behest of the United States, Europe, and other democratic regimes, citing both economic policy and human rights concerns about giving authoritarian regimes excessive control over Internet infrastructure.[12]

Privacy Protection

The commercial, consumer-oriented aspect of the Internet economy is essentially dependent on the intensive use of personal information. Major commercial platforms such as Google and Facebook depend on advertising revenue generated through intensive analysis of users' personal data, and future technologies such as autonomous vehicles and personal health services will all generate even larger amounts of sensitive facts about individual behavior and private lives. Some celebrate this as a source of great economic growth and consumer value, while others decry it as pernicious surveillance capitalism that threatens our democratic values. From the beginning of the commercial Internet there have been calls for governments to address the question of how to protect individual privacy. U.S. and European privacy frameworks illustrate this global debate, evolving together over the last forty years. But while they started from common roots, they have diverged significantly in the development of their respective legal systems. Europe has emphasized strong statements of broadly applicable privacy principles, while the United States has written more sector-specific rules and relied on a large amount of case-by-case exposition.[13]

The strength of the European privacy principle is evident, first and foremost, in the newly adopted Treaty of Lisbon, establishing data protection as a fundamental right for all citizens of the European Union. Meanwhile, in the United States the period from the 1990s to the present has seen intensive implementation of fundamental privacy principles born in the 1960s and 1970s. To begin with, the United States passed a number of new privacy laws, including protection for email and web browsing transactional records, protection of driver's license data, children's online privacy, health information privacy, expanded protections for financial

records, credit data privacy, and genetic information privacy. These laws extend specific privacy protections to a number of different categories of commercial and government activities judged to pose significant privacy risks, and they address consumer protection in key areas of commerce such as consumer credit and financial services.[14]

The United States has one significant gap, however: there is no overarching statutory privacy protection for general commercial activity beyond specifically regulated sectors. This has left the realm of new online services with inadequate protection. Thus, the most robust attention to implementation of privacy principles in the United States has come in the very place where the biggest statutory gap exists.

With the enactment of the General Data Protection Regulation, the EU has become the leading authority on privacy, and the global privacy debate has gone from multipolar (EU, U.S., and Asia) to unipolar. A unique feature of the EU privacy law known as the "adequacy provision" requires that EU citizens' personal data may only be transferred to third countries whose privacy laws have been declared "adequate." Hence, countries around the world must adopt EU-style privacy laws if their companies are to be allowed to do business in Europe. The impact on business from these new rules is far from clear. Going forward, the most challenging questions are likely to arise when established industries, such as finance, insurance, pharmaceuticals, and automobiles, seek to apply personal information–intensive technologies such as machine learning and other forms of artificial intelligence to their products.

Net Neutrality

From the inception of the commercial Internet until 2017, users and service providers have been able to count on some form of legal guarantee of nondiscriminatory access to the Internet in most major markets around the world, allowing a low barrier to entry for new businesses online.[15] Often referred to as "net neutrality," this means that the company providing Internet access would provide connections with all websites or services on the same terms, regardless of the business relationship (or lack thereof) between that service and the communications company. In the 1990s most users in the United States accessed the Internet with dial-up modems, so they took tacit advantage of the fact that telephone companies had to offer nondiscriminatory service under long-standing telecommunications laws. As high-speed Internet access became more common, the U.S.

Federal Communications Commission (FCC) adopted various regulatory approaches, more or less prescriptive depending on the times, but always retained the ability to investigate incidents of discriminatory behavior, at least until 2017. Around the world, some form of nondiscriminatory access expectation has been the norm, and it is widely credited for enabling key innovations on the Internet, including the World Wide Web and the massive economic growth that has accompanied it.

Looking Ahead: Challenges to the Internet's Economic Impact

Technical, social, geopolitical, and public policy circumstances have changed substantially in the more than twenty-five years since the Internet was first opened for commercial use. The foundations of Internet policy presented above were introduced when the Internet was relatively new and optimism about its benefits was infectious. Yet as the Internet has matured, new challenges have sprung up that threaten its success as a domain for pursuing economic prosperity. These challenges are well recognized among technical experts and in popular culture:

- Big data and powerful analytics
- Larger platforms with greater market concentration
- The rise of technically sophisticated authoritarian regimes

Each of these areas of change requires careful examination and perhaps adjustment of one or more of the foundations of Internet policy. In many cases, they suggest the need for more mature and democratically engaged governance processes. If we are to continue to prioritize economic growth as the Internet's prime directive, these new global challenges call for government policy engagement that creates more robust and more democratic institutions that can ensure the Internet economy grows in a manner based on citizen trust and clear, predictable rules for new businesses. At its core, this will mean keeping a clear eye on the contributions made by the original foundations of Internet policy, with well-considered adjustments as called for by an investigation of the current technical and economic landscape.

Big Data and Powerful Analytics

The Internet houses increasingly vast quantities of data about more and more people and accounts for an ever-increasing share of global economic, political, and

https://doi.org/10.1017/S0892679418000606 Published online by Cambridge University Press

personal activity, all of which is today subject to ever more incisive analytics. This data ranges from financial transactions to health status to movement of goods and services in the physical world. Inherent in each of these data categories is an entirely new business sector: financial technology (FinTech) services enabled by more open financial transaction data, personalized healthcare services made possible by better access to fine-grained personal health information, and basic commercial services that bring increased efficiency to sales and marketing practices.

However, the growing universe of data and increasingly powerful analytic capabilities raises the stakes substantially on privacy. New services, especially those that collect sensitive data from users and those that deploy advanced analytics and machine learning techniques to infer sensitive details about people's lives, can only be sustained in the marketplace if consumers trust that misuse of this data will be punished. Today, over 90 percent of U.S. Internet users feel that they have lost control over their personal data.[16] That is not a sound foundation on which to build the data-intensive Internet economy going forward.

While the U.S. sectoral privacy regulatory approach had many advantages in the early Internet commerce era, prioritizing economic growth going forward means that the time has come for governments to step in with a more active, democratically driven voice, laying out a clear set of enforceable rights for individuals and a more predictable set of rules for business. Given changes in EU law and technological advances that enable enormously more intrusive business models, the current situation in the United States looks increasingly unsustainable. At the same time, businesses themselves may choose to lead in the development of new privacy rules out of a strategic recognition that consumer trust is important in the long run. Or they may adopt a more tactical approach based on the expectation that EU privacy rules will predominate against an inconsistent patchwork of different local requirements in various jurisdictions across the United States. Either way, though the principle remains important, the U.S. policy approach to privacy that dominated the first two decades of the Internet market must be revised.

A secondary effect of the advent of big data is governments' efforts to enact data localization rules, which mandate that data used to deliver services in a country must all be stored and processed within the borders of that country. Such laws are enacted in order to protect consumers, encourage local economic activity, or to protect citizens' privacy and keep information out of the reach of foreign intelligence agencies. However, data localization rules can impose unnecessary

inefficiencies on global Internet platforms optimized to deliver data and services on demand around the world. Forcing any given piece of data to be stored within a particular national boundary can raise the costs of platform services on which numerous businesses and individuals depend. Such restrictions can also be unreasonable restraints on trade, disadvantaging service providers purely based on their location. If the Internet is to be a domain for global economic prosperity, data localization laws must be addressed, and a natural way to address them might be through trade agreements that guarantee broad freedom of expression and free flow of information.

For example, the Trans-Pacific Partnership agreement, pursued by President Obama with Pacific Rim allies and then abandoned by President Trump, contained draft provisions limiting harmful data localization requirements. However, because the agreement was negotiated in secret, many consumer advocacy groups opposed its ratification. Civil society organizations were right to worry that such agreements could be harmful to consumer interests, but their concerns could be addressed if the negotiating process were made more transparent and if governments committed to addressing consumer welfare in such agreements as opposed to only creating rules that are of interest to the business community.

As trade agreements are one of the only mechanisms that can address data localization rules on a comprehensive basis, a world that prioritizes cyberspace as being for economic prosperity might see governments developing more transparent, responsive global trade strategies to keep information flowing freely across the globe.

Bigger Platforms with Greater Market Concentration

With the success of the Internet has come greater concentration in the key services and platforms on which much of the rest of the Internet economy, and indeed the economy as a whole, depends. When the U.S. Congress enacted the core suite of foundational Internet policies, there were thousands of Internet Service Providers (ISPs) across the country and a rapidly growing array of websites on which users could post and access content. However, by 2017, fully 85 percent of U.S. Internet users got their broadband Internet access from one of the top five ISPs nationwide, and 80 percent of Internet users had a choice of only two ISPs in their local market. Along with this concentration of access providers, the leading edge platforms—search engines, social networks, cloud providers—also tend to be highly concentrated. Amazon Web Services, the largest provider of cloud

computing services, has 35 percent market share, with its competitors Microsoft, Google, IBM, and Alibaba each at 10 percent or less.[17] Similarly, Facebook holds over 70 percent share of the social networking marketplace in the United States as measured by user time on the platform.[18]

While it is beyond the scope of this essay to consider whether any of these platforms possess market power under antitrust law, there is a clear interest in keeping the market open to new competitors. Strengthening two of the Internet policy foundations can support this goal. First, maintaining some form of nondiscriminatory network access will be vital for enabling new competitors to enter the Internet platform marketplace. Now-powerful services such as Google Search and Amazon Web Services, as well as social networks such as Facebook, were all able to enter the market as new competitors because they were assured nondiscriminatory Internet access. Had Facebook been required to seek permission to operate from the nation's Internet Service Provider it is hard to predict what would have happened, but it certainly would have been an additional barrier to innovation and growth. The United States recently repealed these protections with the FCC's withdrawal of the 2015 net neutrality rules. Restoring net neutrality protections in the United States will require either that the FCC reconsider its nearly total deregulation of Internet access or that Congress enact statutory net neutrality provisions.[19]

Open technical standards are also important to enable new innovators to develop new services that compete with incumbents. As a former upstart that is now dominant, Google Search was only able to grow and thrive because of the open standards that define the World Wide Web. Today and going forward, an Internet environment that prioritizes economic growth first and foremost needs open data standards that create common formats for the information that will be the raw material for new data analytics companies.

The U.K. Open Banking initiative is an example of such a suite of new open data standards.[20] These make it easy for individuals to share banking data with new FinTech services while also adhering to related regulatory requirements that mandate that established financial services companies provide data in the approved open formats. Such open technical standards will be important to promote innovation in a variety of new markets including personal health data, location information, transport services data, information from autonomous vehicles, and many others. More than anything else, the Internet and World Wide Web have shown that open standards allow for the creation of platforms on top of

which innovation can flourish. The challenge going forward is to assure that the data we need for innovation will be open for the next generation of entrepreneurs.

The Rise of Technically Sophisticated Authoritarian Regimes

When the Internet first appeared on the global stage it was regarded by early enthusiasts as a tool against authoritarian regimes because of its ability to give any user access to information from all around the world, including from sources previously forbidden by repressive regimes. Accordingly, authoritarian governments saw the Internet as a threat and not only tried to crack down domestically but also sought the protection of international institutions to guard their prerogative to censor speech and control unwanted outside influence.[21] Russia, in particular, mounted an effort at the United Nations to seek protection from destabilizing influences that might be carried by the Internet.

Yet today, leading nondemocratic regimes such as China and Russia have gone on the offensive, flipping the old power dynamic on its head. China has developed a robust research and industrial policy program supporting many Internet and artificial intelligence–related industries. Chinese authorities have deployed Internet technology to decidedly undemocratic ends, such as by blocking information on the Chinese Internet and using AI analytic techniques to develop a "social credit" system for its entire population. Russia's sophistication with offensive cyber intrusion techniques hardly needs comment, given its now well-understood efforts to destabilize political processes in the United States, France, Germany, and other democratic regimes.

In light of the manifest and strategic technical sophistication of authoritarian regimes, the ongoing commercial viability of the global Internet economy requires the reassertion of several key Internet policy foundations. Excessive, extrajudicial surveillance in large Internet markets puts pressure on global Internet companies that aim to both follow the law in countries where they do business as well as act with respect for global human rights norms. In China, for example, a particularly large and lucrative market, companies are pressured to abide by local censorship and surveillance rules even when they fall short of international human rights standards. This highlights a need to reemphasize both the norm of free expression as well as the fact that rights-based regulation of government surveillance is required by international human rights law and treaty and so should be the norm for all Internet activity. Authoritarian regimes have taken particular advantage of Internet platforms to carry out government censorship and surveillance

outside the rule of law. Putting platforms in the position of having either to violate the human rights of their users or to avoid doing business in a country is an untenable situation. Democratic, free-market countries around the world should recognize this threat to free expression, privacy, and innovation and insist that all countries who benefit from the Internet should abide by basic platform neutrality and liability limitation.

Internet users also express real worry, especially regarding privacy and security, about the trustworthiness of the environment. This lack of trust will gradually erode the stability of the Internet marketplace, causing harm to innovation and economic growth. That is why in a world where cyberspace exists primarily to serve economic interests the laws of major Internet economies would be updated to establish clear privacy rights for individuals that can be enforced in a flexible manner when faced with technical and business model changes. Internet users would be assured that government surveillance is conducted in an accountable fashion under the supervision of an independent judiciary. Such a system would be the best way to protect public safety while also avoiding users having to worry that private companies have become agents of the surveillance state.

Conclusion

The Internet's six technology policy foundations—free expression, intermediary liability limitation, protection against unfettered government surveillance, open technical and operating standards, consumer privacy, and net neutrality—have all been part of enabling the Internet economy to develop around the world. If the prime directive of cyberspace is to bring continued economic prosperity across the globe, these original six foundations will remain just as vital and, indeed, will require additional protections in the face of new challenges. There are currently gaps in the regulatory framework governing the Internet. Maintaining open technical standards and nondiscriminatory Internet access services according to net neutrality principles is vital to avoiding roadblocks that might allow today's incumbents to thwart tomorrow's innovators. Threats to the free flow of information should be met with strong support for freedom of expression and continued liability limitations for Internet platforms. Privacy protection, and cybersecurity along with it, also requires additional action by governments. We face a deficit of public trust around the world, which demands stronger, more effective government authority to protect individual rights and to hold companies to a high

standard of respect for their users' interests. Finding this balance may not be easy, but it is essential to maintaining a trustworthy environment for the next generation of Internet innovation to flourish.

NOTES

[1] Richard Adler, "Toward a Better Understanding of Internet Economics," Richard Paul Richman Center for Business, Law, and Public Policy, June 19, 2018, p. 4, cdn1.internetassociation.org/wp-content/uploads/2018/06/IA-Toward-A-Better-Understanding-Of-Internet-Economics-2018-1.pdf.

[2] Vinton Cerf, "The Internet Is for Everyone," Request for Comments: 3271, Internet Society Memo, April 2002, tools.ietf.org/html/rfc3271.

[3] The first major challenge to the free flow of information on the Internet came as the World Wide Web was achieving rapidly growing levels of use across the United States and the world. It became clear that, along with the many valuable sources of information on the Web, there was also material that was inappropriate for minors. The U.S. Congress soon felt compelled to act to protect children from sexually explicit content online, and so enacted a law known as the Communications Decency Act, which made it a crime to make such material available to minors. Immediately upon enactment, a large coalition of civil liberties organizations, leading technology companies (Microsoft, Apple, America Online), news organizations, and libraries all came together to challenge the law as a threat to free expression online and to the very viability of the Internet. These organizations were not seeking to protect access to pornography, but rather to be sure that the broadest possible First Amendment protections applied to the new medium they were hoping to build. The U.S. Supreme Court struck down the law, finding that the Internet is "a unique and wholly new medium of worldwide human communication. . . . As the most participatory form of mass speech yet developed, the Internet deserves the highest protection from governmental intrusion." *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997).

[4] In U.S. law the two key components of this Internet policy foundation are a general liability limitation known by its legal shorthand as "Section 230" and an online copyright statute known as the Digital Millennium Copyright Act (DMCA). Section 230 relieves platforms of responsibility for harm arising out of content created by a user, as opposed to the platform itself. The DMCA establishes a so-called notice-and-takedown system under which platforms can avoid vicarious copyright liability for their users' postings if they remove allegedly infringing material upon notice from the copyright owner. 47 USC § 230; 17 USC § 512 et seq. Section 230 was enacted along with legislation that banned sexually explicit speech accessible to minors. That censorship component of the law was struck down by the United States Supreme Court in *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997).

[5] Organisation for Economic Co-operation and Development, "OECD Principles for Internet Policy Making" (2014), Annex, p. 16, www.oecd.org/sti/ieconomy/oecd-principles-for-internet-policy-making.pdf.

[6] 47 USC § 230(b)(3)–(4).

[7] J. B. Morris, Jr., and Cynthia M. Wong, "Revisiting User Control: The Emergence and Success of a First Amendment Theory for the Internet Age," *First Amendment Law Review* 8 (2009), pp. 109–38.

[8] 18 USC § 2701 et seq.

[9] European Convention on Human Rights, Articles 7 and 8.

[10] Harold Abelson et al., "Keys under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications," *Journal of Cybersecurity* 1, no. 1 (2015), pp. 69–79.

[11] Laura DeNardis, *The Global War for Internet Governance* (New Haven: Yale University Press, 2014), p. 22.

[12] Kenneth Neil Cukier, "Rich Man, Poor Man: The Geopolitics of Internet Policy Making," in *INET Conferences*, 1998.

[13] For a summary of the legal situation in the United States and Europe, see generally Jean-François Abramatic et al., "Privacy Bridges: EU and US Privacy Experts in Search of Transatlantic Privacy Solutions," 37th International Privacy Conference, Amsterdam (2015), privacybridges.mit.edu/sites/default/files/documents/PrivacyBridges-FINAL.pdf.

[14] See generally Daniel J. Weitzner, "Privacy for a Global Information Society: High Standards, Global Cooperation, Flexibility for the Future," in Hielke Hijmans and Herke Kranenborg, eds., *Data Protection Anno 2014: How to Restore Trust? Contributions in Honour of Peter Hustinx, European Data Protection Supervisor (2004–2014)* (Cambridge, U.K.: Intersentia, 2014), pp. 237–52.

[15] Federal Communications Commission (FCC), Restoring Internet Freedom Order (2017).

[16] Mary Madden et al., "Public Perceptions of Privacy and Security in the Post-Snowden Era," Pew Research Center, November 12, 2014, p. 3, assets.pewresearch.org/wp-content/uploads/sites/14/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf.
[17] Jordan Novet, "Microsoft Narrows Amazon's Lead in Cloud, but the Gap Remains Large," *CNBC*, April 27, 2018, www.cnbc.com/2018/04/27/microsoft-gains-cloud-market-share-in-q1-but-aws-still-dominates.html.
[18] ComScore Social Media Share of Time 2018, www.smartinsights.com/digital-marketing-strategy/popular-social-networks-worldwide-chartoftheday/attachment/social-media-network-popularity-2018/.
[19] For a review of various national approaches to net neutrality see Christopher T. Marsden, *Network Neutrality: From Policy to Law to Regulation* (Manchester: Manchester University Press, 2017).
[20] See www.openbanking.org.uk/.
[21] United Nations General Assembly, "International Code of Conduct for Information Security," in "Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations," A/66/359, September 14, 2011.

Abstract: Unique among major communications media, the Internet has delivered vast public benefit while being designed, developed, and deployed largely through private initiative and nongovernmental funding. At the same time, key public policy decisions were made early on that established the legal and regulatory foundations necessary for economic innovation and free expression to flourish. Those foundations include strong free speech protections, liability limits on Internet platforms, protections against excessive government surveillance, open technical standards, individual privacy protection, and some form of net neutrality. Those foundations were laid when the Internet was young. As part of a roundtable on "Competing Visions for Cyberspace," this essay argues that as the business, social, and technical impact of the Internet has become clearer globally, some of these principles require adjustment, but all will remain important if we are to preserve the economic potential of the Internet environment going forward.

Keywords: Internet policy, privacy, free flow of information, economic innovation, free speech, net neutrality, economics, cyberspace