BRILL

PROTEST 4 (2024) 279–288

PROTEST
brill.com/prot

Book Review

Jeffrey A. Hart (2023), *Essays on the History and Politics of the Internet: Cyberpolitics*. Newcastle upon Tyne, UK: Cambridge Scholars Publishing. xvi + 192 pp., ISBN: 978-1-5275-2870-3.

The Internet is one of the most pervasive aspects of modern life. From the Arab Spring to Gezi Park protests in Turkey, Occupy Wall Street and Black Lives Matter in the US, Yellow Vests in France, RickyLeaks in Puerto Rico, Hong Kong protests, and beyond, the Internet has been instrumental in shaping social movement activism in recent years. Protest movements in our times have all benefitted from the interconnectivity and interactive networks afforded by the Internet. It is thanks to the Internet that social movement activists are able to bypass the confines and restrictions imposed on dissent and civic organizing by those ensconced in the corridors of power. But the Internet is a double-edged sword. Authoritarian governments also use the Internet for surveillance and gathering intelligence, tracking down and hunting dissidents, foiling and squashing protests, and propagandizing and ensuring that the government's line reigns supreme in public discourse. In many ways, the centrality of digital activism to social movements and tyrants alike is indicative of how the Internet and modern technologies have transformed our lives and the way we do things: from protests, civic mobilization, political participation, and social control down to, *inter alia*, learning, managing finances, commerce, shopping, and accessing entertainment.

While most people around the globe use the Internet in one way or another, only a small number know how the Internet has come about and developed. In his *Essays on the History and Politics of the Internet: Cyberpolitics*, Jeffrey A. Hart sets out to provide a comprehensive, yet concise, primer on the history and impact of the Internet for specialists and non-specialists alike. A political scientist by profession, Hart's narrative is preoccupied with the implications of the Internet's development and rise to ubiquity for the distribution of power in society and internationally. From the start, the author makes clear

Published with license by Koninklijke Brill BV | DOI:10.1163/2667372X-BJA10063
© KHALIL FADL OSMAN, 2024 | ISSN: 2667-3711 (print) 2667-372X (online)

that a major theme explored in his book is the stark gap between the current reality of the Internet and the democratic dream of universal empowerment envisioned by the creators of the Internet. "The current reality is different," Hart laments. Different answers have been given to explain how and why this contrast came about. Some "believe that the Internet simply preserves or even reinforces preexisting power structures. Others believe that it has the potential to increase inequality and to strengthen the hand of central governments and large corporations" (p. xvi).

Hart traces the genesis of the Internet to the efforts of scientists, such as J.C.R. Licklider and Robert Taylor, at the Advanced Research Projects Agency (ARPA) of the US Department of Defense in the early 1960s aiming to "accelerate the development of time-sharing computers and computer networks" (p. 2). These efforts built on earlier work by Paul Baran at the Rand Corporation in the 1950s to create a robust communications system capable of surviving a nuclear first strike. Clearly, Cold War anxieties weighed down heavily on the work to develop such communications systems. These were times when the principle of "mutual assured destruction" (MAD) constituted the fulcrum on which US military and national security doctrine rested. The MAD principle was premised on surviving a first nuclear strike to be able to deal a second strike to the attacker, thus ensuring the annihilation of both attacker and defender. The logic of the MAD strategy would work only if the US, after coming under a first nuclear strike, could retain the efficient military communications system necessary to direct a second, retaliatory nuclear strike.

Subsequent research funded by US government and corporate sources would culminate in the building of ARPANET in 1969, which linked computers in an expanding network of US defense agencies, defense contractors, and academics. While computer scientists who comprised most ARPANET users used the network to exchange electronic mails, they "later put pressure on the Department of Defense to provide broader access to realize its full potential for the scientific community" (p. 6). At the same time, other special purpose networks began to appear, developed by corporate and industrial entities "to give access to electronic mail capabilities to non-defense-contracting computer science and academic communities respectively" (pp. 6–7). A noteworthy development in this regard is the building of the NSFNET by the National Science Foundation in 1988. Mounting competition and lobbying by academic and corporate interests would contribute to the Department of Defense's decision in October 1983 to "officially split [the ARPANET] into two networks: MILNET [devoted for military communication] and the "residual" ARPANET" for general use (p. 9). The rapid growth of traffic on the NSFNET would render the residual ARPANET obsolete. As a result, the network was decommissioned

in 1990. "The ARPANET had served its purpose well," Hart explains, "but was not able to become the backbone for the new NSFNET because it was too slow. The visions behind the NSFNET and the Internet were more expansive and inclusive" (p. 12).

While these developments unfolded, Hart's narrative shows, the original national security and elitist academic vision of network usage was becoming progressively wedded to a commercial business, yet egalitarian, vision that sought to upgrade the Internet backbone. This was fueled by interest in developing new information resources to roll back the erosion of America's international competitiveness. Spearheaded by the efforts of Senator Albert Gore, proponents of this vision argued that this could be achieved "not just by improving the telecommunications infrastructure for academic and business research, but also by helping to develop new information resources for K-12 education [i.e., education from kindergarten through high school] and the public at large" (p. 16). Gore's efforts came to fruition with the passage into law of the High-Performance Computing and National Research and Education Network Act on September 11, 1991. The law required the White House to report to Congress on activities by the federal government to promote supercomputing and high-speed networking. More importantly, it included authorized federal funding for research on supercomputing and high-speed networking. However, in practice, as Hart maintains, the implementation of this legislation did not reflect the egalitarian vision of Gore and others which privileges universal network access but rather the ivory-tower vision of academics and their obsession with "Grand Challenges" in science and technology. As Hart states: "There were no gigabit applications dealing with interconnection of libraries or creating easy-to-use interfaces for gigabit applications for the general public. Most of the gigabit applications reflect "big science" priorities in medicine, chemistry, earth sciences, meteorology, seismology, and 3-D visualization" (p. 23).

The transition to a more democratic vision of Internet access would have to wait for the creation of the World Wide Web and the emergence of relatively affordable personal computers and smartphones. Hart argues that this transition was driven by the corporate desire for financial gain. Several factors converged to propel the steep rise in Internet access and use. Technological advances in both hardware and software enabled users to create and share content. This was facilitated by the removal of access barriers by governments. As Hart explains, before commercialization, users mainly used the Internet for email and file sharing, primarily text and images. However, the creation of the World Wide Web, due in large part to the work of Geneva-based and British researchers and political scientists, made it easier to access information

and engage in business transactions via the Internet. Traffic increased progressively with the appearance of new inventions such as free and public domain browser software, fiber optic technology, broadband networks, and wireless technology, which would enable cell phones to handle email and access websites. According to Hart, a key aspect of the commercialization of the Internet which contributed to the rise in traffic in the US has been "the increased competition between the various local and long distance carriers [which] resulted in lower rates for consumers" (p. 36). Regulatory changes, which enabled cable television companies to provide telephone and Internet services, intensified competition and facilitated investments in infrastructure that boosted dial-up and broadband services.

As the Internet took hold, it fell short of the unreservedly democratic ideals and universal empowerment envisioned by its creators. Inequality in access to the Internet across and within nations restricted the possibility of turning cyberspace into a full-scale electronic agora. This came to be known as the "digital divide." In describing this multifaceted phenomenon, Hart states that "the divide is not a singular phenomenon but exists across a variety of groups: for example, urban vs. rural communities, groups with differing levels of income and education, and different ethnic and racial groups" (p. 41). He links this differential empowerment to three factors: availability of actual access to the Internet; adeptness at using the devices that provide access and efficiently processing the information obtained through the Internet; and ability to incorporate the obtained information in activities that produce positive results.

The digital divide mirrors existing inequalities, and, accordingly, it is a multilayered gap. On the international level, for example, there is a gap between developed and developing poor countries. There is also a gap between lower income developing countries and higher income ones. "This," Hart explains, "may be a result of a higher percentage of rural inhabitants and of people with lower income and less education. In addition, access to mobile phones is more limited and more expensive in poor countries and the prices of computers and telephones may also be higher than in richer countries. Access to stable electrical power and batteries may also be limited" (p. 43). Similar stratification exists within nations. For example, "[e]thnic and racial differences in access to the internet persisted" in the US. "Blacks, Latinos, and Native Americans were much less likely than Whites and Asians to have a computer at home or to have a broadband connection" (p. 44).

Gaps in Internet penetration exist between rural and urban communities worldwide. This has placed children in poorer countries, as well as children

of racial and ethnic minorities in rich countries, at a particular disadvantage during the COVID-19 pandemic when many schools transitioned to e-learning. Beyond physical access, Hart notes, the lack of digital skills among some segments of the population – the elderly, for example – causes some "people who have access in theory to the Internet [to] choose not to make use of it" (p. 50). Another aspect of the digital divide stems from the disparities and variations in digital skills between individuals. While nearly all Internet users use the network to obtain information and communicate with others, a smaller subgroup can use it to create and upload content or to achieve other personal goals.

Hart surveys international and national efforts to bridge the digital divide. For example, the Okinawa Charter on the Global Information Society adopted at a Group of Eight summit in July 2000 embraced, *inter alia*, the goal of inclusion, specifying that "everyone, everywhere should be enabled to participate in and no one should be excluded from the benefits of the global information society" (p. 52). The author also discusses national efforts by several countries to bridge the digital divide, such as the creation of the Connect America Fund in October 2011 to provide broadband Internet service to inadequately served communities in the US, the European Union's Digital Agenda for Europe adopted in 2010, and Chinese and Indian initiatives to bridge the rural-urban divide. Hart's survey of these efforts leads him to a sobering, yet disheartening, conclusion. "Progress toward bridging the digital divide," he writes, "has been limited by underinvestment in infrastructure and education programs for digital skills. Divides based on location, age, income, gender, and levels of education remain to be closed. Recognition of the importance of providing universal access to broadband services and upgrading the capacity of individuals and groups to use those services has increased, especially in the wake of the COVID pandemic. Even the wealthiest countries have not succeeded in closing the gap. For this reason, bridging the digital divide will remain an important political issue for the foreseeable future" (p. 56).

Translating the democratic vision of universal access to the Internet into reality was also complicated by the ability of providers to interfere with, even block, the movement of information. Owners of Internet infrastructure, including commercial providers, had an incentive to prioritize the delivery of certain content. For example, cable TV providers have an incentive to privilege the delivery of video content or to restrict the delivery of video content produced by their competitors. "Governments," moreover, "may want to restrict the flow of information that violates laws against child pornography, intellectual property theft, or other content deemed inappropriate" (p. 57). The turn of the

millennium saw a heated debate in the US over guaranteeing so-called "net neutrality," i.e., instituting safeguards to ensure nondiscrimination by owners of Internet wires or "pipes" against Internet content of the same nature. Hart treats his readers to a vivid examination of this controversy which unfolded in the US along the lines of the traditional American debate over government regulation and free speech. Proponents argued that instituting safeguards to ensure nondiscrimination was "important from the perspective of preserving freedom of speech and preventing censorship of unpopular ideas" (p. 59). On the other hand, opponents of net neutrality, who included telephone and telecommunications companies and their conservative political supporters, argued that government regulations to ensure net neutrality would discourage corporate investments in broadband infrastructure which would, in turn, have an adverse impact on the development of the Internet. Through his examination of this debate, Hart weaves an account of how net neutrality rules were instituted in the US and Europe to protect the rights of the public to access information and services via the Internet.

From a libertarian standpoint, however heartening the debate over net neutrality might be, Hart's discussion of surveillance in Chapter 5 is disheartening, to say the least. Despite all its much-ballyhooed democratic promises, the Internet, and information and communication technology (ICT) in general, can be used for oppressive purposes, including increasing the government's surveillance capabilities over citizens. As Hart aptly notes, concerns over the increased use of electronic surveillance by governments heightened following the September 11 attacks. Intelligence failures in preventing the attacks fueled the US government's tendency to boost the capabilities of the intelligence community "to detect and apprehend potential terrorists inside the United States." This invigorated drive included expanding the use of data mining technologies which "employ advanced computers and computer software to identify patterns that are not easily discerned by other methods. Data mining goes beyond data collection, access, and analysis by applying computer algorithms to detect patterns across linked databases" (p. 105). According to Hart, the US government had started using data mining in the early 1990s to detect and clamp down on money laundering and screen airline passengers. By the late 1990s, the US Special Operations Command had begun to experiment with the "mining of both classified and open-source information to identify potential terrorists and terrorist operations" (p. 107).

Hart offers an extensive review of several data mining and warrantless wiretapping initiatives and programs introduced by the US defense and security establishment in a bid to apply information technology to counter transnational security, especially terrorist, threats as well as the controversies

that have swirled around these policies. The adoption of these policies was met with opposition by civil libertarians who expressed deep concerns about lack of transparency, invasion of privacy, putting US citizens under surveillance, and the potential for the abuse of collected data by corporate and government entities. Hart's account shows that opposition by civil liberties groups and in Congress forced the US government to cancel and discontinue some surveillance programs, such as the Department of Homeland Security's Computer-Assisted Passenger Screening System (CAPPS II). However, other surveillance programs, many of which are clandestine, as disclosed by Edward Snowden, including the National Security Agency's surveillance program codenamed PRISM which collects and process data from private and government sources, continued. Hart also provides a fast-paced survey of digital surveillance in China and Russia.

Hart points out that rising concerns in the US about government surveillance after September 11 have been compounded by concerns about "surveillance capitalism," i.e., the amassing, storage, and processing of gargantuan pools of personal data by private companies without seeking the permission of the individuals about whom the data is collected. "Unlike industrial capitalism," Hart writes, "which exploits natural resources and cheap labor to profit from investments by producing goods and services, surveillance capitalism captures behavioral data and then sells analysis of those data to advertisers and other customers" (p. 121).

The controversy about surveillance is part of a broader debate about balancing the requirements of security with constitutional guarantees and laws regarding privacy protection and civil liberties. It underscores the tensions between supporting civil liberties and maintaining security. Seen from the angle of surveillance proponents, the debate raises a question about the extent to which "legal privacy protections necessarily impair national security" (p. 123). This debate calls to mind the dilemma of counterterrorism and liberal democracy, whereby overly militaristic and repressive counterterrorism measures in a democratic state may lead to the erosion of its liberal democratic character (Wilkinson, 1977 and 2011). Hart maintains that such controversies, and the dilemmas underlying them, underscore the "need to rethink the rules governing the ownership and control over information and information flows" (p. 124).

The rapid growth of the Internet has also given rise to concerns about potential infringement of intellectual property rights. Digital technology makes it easier, cheaper, and faster to copy and share text, audio, video and other content with minimal reduction in quality. Hart draws on a wide array of sources to construct a portrait of the development of US copyright

laws since the early days of the American republic. He surveys the lobbying efforts spearheaded by the recording and film industries to secure legislation providing for the shutdown of websites both inside the US and abroad on grounds of infringement of US copyrights and selling counterfeit goods. His survey includes a painstaking and detailed examination of the failure of lobbying efforts to pass two landmark proposed bills, the Protect Intellectual Property Act (PIPA) and the Stop Online Piracy Act (SOPA), in Congress. He shows how these efforts foundered on the rock of opposition by opponents concerned about the two bills' "potential for censorship and other restrictions on free speech" (p. 125). An interesting aspect of this episode is the opponents' use of the Internet to mobilize the public against both proposed legislations, eventually forcing even many congressional sponsors to switch position and vote against them. Ultimately, the two proposed bills were shelved, providing "a dramatic example of how people power can defeat moneyed interests" (p. 154).

The relationship between the Internet and power animates Hart's book. "The politics of the Internet," he loudly proclaims, "centers on questions of power" (p. 155). Hart is especially concerned about the effects of the diffusion of ICTs on the empowerment of individuals, small and large organizations and institutions, governments, corporations, nations, and other human collectivities and social strata. A central question here revolves around how these technologies subvert or reinforce domestic and international power hierarchies and relations.

In a chapter that zeroes in on the questions of power swirling around the politics of the Internet, Hart takes his readers on an excursus into the contending conceptions of power in political science. Against this backdrop, he provides a brief assessment of the impact of the diffusion of ICTs, including the Internet, on domestic and international distributions of power from the perspective of three main approaches to the empirical measurement of power: "1) power as a resource or capability, 2) power as a relationship, and 3) power as a structure" (p. 162). Assessing and measuring power in terms of ICT capabilities, he points out, would focus on indicators such as "national investments in research and development (R&D), numbers of scientists and researchers, and patenting activity" (p. 163). From this perspective, the inventory of ICT capabilities that is taken into consideration includes the country's role in the production and marketing of ICT-related products and services, the citizens' access to technology, and "the number of landline and cellular telephones and Internet users and Internet hosts" (p. 165). Undergirding this assumption is an unescapable classical realist view that these power resources are fungible and can be translated into actual power and influence. Notwithstanding the fact

that this view has come to be largely stale and obsolete in academic circles, it has continued to animate the heated policy debates in the US on such issues as the domestic broadband infrastructure and US-China relations, as evidenced by the controversy over TikTok. Hart emphasizes that while other industrialized nations have surpassed the US in some areas of ICT business activities, "US firms remain powerful and sometimes dominant players in key areas," including the design of microprocessors and the production of software and PC operating systems. He notes that this phenomenon calls attention to "a new form of power peculiar to ICTs: the power to determine technical aspects of an ICT *platform* or *architecture*" (pp. 166–167, emphasis in original).

On the other hand, the measurement of ICTs from the relational power perspective directs attention to the distribution of power between individuals and institutions, including governments and multinational corporations. In this context, Hart refers to the work of authors such as John Perry Barlow who argue "that individual users will push hard for minimal barriers to access once they see the potential for free speech and individual empowerment" made possible by the Internet. However, Hart shows that the picture is not straightforward as evidenced by the work of authors such as Lawrence Lessig who argue that "the technology itself has the potential to either empower individuals or to empower large institutions." Accordingly, absent guarantees and safeguards to protect individual rights, "ICTs make it easier and cheaper for governments and corporations to spy on individuals and to act against those they consider to be threats" (p. 169). Moreover, ICTs have also had an impact on relational power at the international level. They enable transnational social movements to publicize and advocate for their causes, raise funds, recruit, mobilize, and plan and organize activities. At the same time, the development of ICTs has created opportunities for "the use of information technology as an alternative to or in addition to military force" (p. 171). Hart points to the increased interest of state and non-state actors in deploying ICTs as tools of cyberwarfare whereby cyber-attacks are launched against the military installations, information systems, economic operations, power generation grids, transportation systems and other targets in an enemy entity with as eye to disrupt or inflict damage on its military capabilities, economic base, information flows, and infrastructure.

Finally, Harts discusses the impact of ICTs on the larger set of rules, norms and procedures governing the international system. Influencing these normative underpinnings of the international system is an indicator of structural power. Hart argues that since ICTs "embed institutional and cultural practices into the technology itself … a certain amount of structural power is implicit in the transfer of information technologies across national boundaries" (p. 172). This empowers the nations that produce and market ICTs

to impose their institutional and cultural frameworks and norms on others. In this regard, Hart cites the dominance of American corporations, such as Microsoft, Intel and Google, in desktop operating systems, microprocessors, smart phones, search engines, and online advertising. He states that "ICT companies and users in Europe and Asia have tried to compete with these firms but with limited success and now are forced to adapt to the technological solutions that the dominant firms have imposed on them (as well as the rest of the world)" (p. 173).

Hart concludes this discussion by stressing that the theories and conceptions of power in political science have yet to catch up with the impact of the fast and radical changes in ICT s on the distribution of power. Arguing that the political science literature is largely oblivious to how technology and technological architectures shape the distribution of power, he calls for making "important modifications in received notions of power … in order to successfully apply the lessons of power analysis to ICT-related activities." He further notes that "whereas control over conventional resources is often a zero-sum game, control over informational and cultural resources may be less dangerous and destructive than rivalries that center on territory or economic growth" (p. 174).

Overall, Hart's book constructs a comprehensive, yet brief, account of the history and political implications of the Internet. It is academic, informative, timely and enjoyable, at one and the same time. Hart is rigorous in presenting his cogent arguments. His simple style and lucid presentation make the book highly readable for a wide range of audiences, including academic scholars, practitioners and non-experts alike. His book is a must-read for those interested in or puzzled by the ubiquity of ICT s in our lives and how it has been affecting the distribution of power in societies and globally.

Khalil Fadl Osman
Senior Research Fellow, Center for Conflict and Humanitarian Studies, Doha, Qatar
khalil.osman@chs-doha.org

References

Wilkinson, Paul (1977). *Terrorism and the Liberal State*. London: Macmillan.

Wilkinson, Paul (2011). *Terrorism versus Democracy: The Liberal State Response*, 3rd Edition. London: Routledge.