Degrees of Freedom, Dimensions of Power

Yochai Benkler

Abstract: The original Internet design combined technical, organizational, and cultural characteristics that decentralized power along diverse dimensions. Decentralized institutional, technical, and market power maximized freedom to operate and innovate at the expense of control. Market developments have introduced new points of control. Mobile and cloud computing, the Internet of Things, fiber transition, big data, surveillance, and behavioral marketing introduce new control points and dimensions of power into the Internet as a social-cultural-economic platform. Unlike in the Internet's first generation, companies and governments are well aware of the significance of design choices, and are jostling to acquire power over, and appropriate value from, networked activity. If we are to preserve the democratic and creative promise of the Internet, we must continuously diagnose control points as they emerge and devise mechanisms of recreating diversity of constraint and degrees of freedom in the network to work around these forms of reconcentrated power.

YOCHAI BENKLER is the Berkman Professor of Entrepreneurial Legal Studies at Harvard Law School, and serves as Faculty Co-Director of the Berkman Center for Internet and Society at Harvard University. He is the author of *The Wealth of Networks: How Social Production Transforms Markets and Freedom* (2006), which won awards from the American Sociological Association and the American Political Science Association.

In March 2000, AOL tried to pull a program that two of its employees had released online twenty-four hours earlier. Gnutella was a peer-to-peer file sharing program, and AOL was concerned about copyright liability. But Gnutella was free software, and it had been released, along with its source code, under the GNU General Public License. Gnutella was quickly adopted and developed by diverse groups, becoming the basis for a range of peer-to-peer (P2P) networks that either used or improved upon its source code. Technical architecture, cultural practice, social production, market structure, and timing had prevented AOL from halting the development of Gnutella.

Fourteen years later, in February 2014, Apple's app store rejected a game that mocked North Korean leader Kim Jong Un. Apple already had a history of blocking applications of which it disapproved: cartoons that mocked President Obama, an app for browsing State Department cables on WikiLeaks, or a game that criticized the company's treatment of its workers in iPhone manufacturing processes. Initially, Apple had also forced Skype to block usage on 3G mobile networks, rejected the Google Voice app, and disabled Google Maps on the iPhone. Here developments en-

doi:10.1162/DAED_a_00362

abled Apple to exert power over users and developers in a manner that was simply impossible a decade and a half earlier: smartphones running over proprietary cellular networks, an operating system integrated with hardware that controlled what software is preloaded and made available, and an "app store" model of software distribution.

In 1993, *The New Yorker* published a Peter Steiner cartoon with the caption, "On the Internet, nobody knows you're a dog." By 2014, Maidan protesters in Kiev could receive text messages that read, "Dear subscriber, you are registered as a participant in a mass disturbance."[1] Whether Internet design ultimately will support a high degree of freedom, as was offered by the first generation Internet, or will evolve toward a system that amplifies power in the hands of the state and a concentrated class of private actors, is the central design challenge of the coming decade.

In its first quarter-century, "the Internet" was not only a technical system, but also an innovative organizational system; an institutional system pervaded by commons; a competitive market with low barriers to entry; and, finally, a zeitgeist, cultural habit of mind, or ideology, perhaps best captured by the saying from computer scientist and early architect of the Internet, David Clark: "We reject: kings, presidents and voting. We believe in: rough consensus and running code."[2] It is the integrated effect of all these dimensions that should properly be understood as the Internet in its first twenty-five years, and it is changes in several of these elements that underwrite the transformation of the Internet into a more effective platform for the reconcentration of power.

The introduction of the iPhone in 2007 marked the shift to handheld computing and ushered in a shift to proprietary, controlled devices, software, and networks. Amazon's Elastic Compute Cloud (EC2) – introduced in 2006 – created another potential point of control. The coming of age of advertiser-supported platforms and the emergence, in 2008, of "big data" as both a working concept and catchphrase marked a new drive to collect data and deploy it. Big data may ultimately allow a small number of companies – those large enough to control, access, and analyze sufficient data – to predict, shape, and "nudge" the behaviors of hundreds of millions of people. Since the mid-2000s, home broadband has been replicating some of telecommunications' older monopoly characteristics, while ever-higher speeds are shifting usage further toward streaming video. Consumer demand for high-grade commercial video services, most prominently Netflix, has in turn increased the pressure to implement technical control measures in basic infrastructure, capped by the adoption of Digital Rights Management (DRM) as a core component of HTML5 in 2014. Together, these changes have destabilized the diverse open systems that had made up what we thought of as the Internet.

The design of the original Internet was biased in favor of decentralization of power and freedom to act. As a result, we benefited from an explosion of decentralized entrepreneurial activity and expressive individual work, as well as extensive participatory activity. But the design characteristics that underwrote these gains also supported cybercrime, spam, and malice.

By *power*, I mean the capacity of an entity to alter the behaviors, beliefs, outcomes, or configurations of some other entity. Power, in itself, is not good or bad; centralization and decentralization are not good or bad, in and of themselves. Centralized power may be in the hands of the state (legitimate or authoritarian) or big companies (responsive and efficient or extractive), and decentralized power may be distributed among individuals (participating citizens, expressive users, entrepreneurs, or criminals) or

loose collectives (engaged crowds or wild mobs). To imagine either that all centralized power is good and all decentralized power is criminal and mob-like, or that all decentralized power is participatory and expressive and all centralized power is extractive and authoritarian is wildly ahistorical.

Internet architecture shapes power, and unlike in the early days, everyone knows this now. Because power often involves the capacity to reshape terms of engagement, we are seeing extensive efforts to lock and extend existing power. If one were naive enough to imagine that all efforts at centralization were aimed merely at taming the "bad" decentralization, one might be sanguine about the fact that governments and companies are pushing toward greater centralization. Further, if one is paranoid enough to imagine that decentralization necessarily resolves to mob rule, then a similar sanguinity is called for. But in the absence of these assumptions, we are left with the task of maintaining an Internet both open enough and resistant enough to power to allow, at least, continued contestation of decisions to create points of control in the networked environment. If we allow that power can be good or bad, whether centralized or decentralized, and that existing dynamics are tending toward greater centralization and stabilization of power, then we are left with a singular task: to design a system that will disrupt forms of power – old and new – as they emerge, and that will provide a range of degrees of freedom, allowing individuals and groups to bob and weave among the sources and forms of power that the Internet is coming to instantiate.

That the original TCP/IP protocol outlines an open, loosely coupled system is, at this point, trivial. The basic end-to-end design principle it instantiates allows any application developer to use the networking protocol to send its payload, whatever that is, to its destination, wherever that may be, on a best-efforts basis. The generality of the protocol disabled crisp identification of the nature of parties to a communication, and offered no control points through which an entity could exclude or constrain another discrete entity attempting to use it. While the Internet protocol itself was a critical element, it was not, by itself, sufficient to diffuse power.

What typified the first quarter-century of the Internet was an integrated system of open systems. These included: the technical standards of the Internet and the World Wide Web; the decentralized, open organizational models of the Internet Engineering Task Force (IETF) and the World Wide Web Consortium (W3C); and the competitive market structure for connectivity (the low cost of copper wire, subject to common carriage rules, resulted in over five thousand Internet service providers, or ISPs) and devices (PCs became a commodity item). These systems were complemented by widespread use of open, standards-based devices (such as PCs running software developed and distributed by a diverse range of entities); the emergence of commons-based production, particularly free and open-source software (FOSS); and the culture of openness and resistance to authority shared by most early users and developers of components of the Internet ecosystem and its core applications. Together, these created a system designed to resist the application of power from any centralized authority, whether it pertained to free speech or to free innovation without permission, which was very much at the core of the Internet's architectural design principles.

Several developments suggest that we are shifting to an Internet that facilitates the accumulation of power by a relatively small set of influential state and nonstate actors. While the Internet protocol itself remains

open, as does the IETF, other control points counter the dynamics of the early Internet.

The first is the emergence of smartphones and the iOS app store. By the middle of 2014, Internet access by smartphone had surpassed Internet access from desktops or laptops.[3] Handheld and tablet users overwhelmingly used apps, rather than browser-based Internet access (Internet access via apps constituted 88 percent of handheld use and 82 percent of tablet use), and the growth rate of desktop use was 1 percent per year, while mobile app use grew more than 50 percent. Unless something dramatic changes these trends, the future of conscious Internet use is based in handheld devices running apps. Moreover, as connected sensors and controllers (origin of the "Internet of Things" as a concept) become pervasive, an increasingly larger portion of Internet use will not be conscious at all. The general-purpose device – owned and managed by its user and capable of running any software from any source – will continue to serve the portion of the population particularly interested in preserving its computational autonomy and in executing more challenging and complex tasks. But, as legal scholar Jonathan Zittrain warned in 2008, the majority of Internet-mediated practice will be undertaken with devices that are either narrowly customizable appliances or controlled on the app store model.[4]

The primary source of constraint on the Apple app store's center of power is competition from Android. In principle, Android OS (operating system) phones can use app stores other than Google's, and relatively simple alteration of the default settings allows users to sideload apps without the app store. In practice, while reliable numbers are scant, it appears that most Android apps are downloaded from Google Play or Amazon's app store. Habits of use and consumer convenience seem to largely negate the effects of the technical feasibility of sideloading. Limits, if any, on the power of the app store owners come from market competition between iOS and Android, and – perhaps, to the extent these constraints exist and are, further, given voice in the organizational cultures of these companies – from internal ethical or cultural constraints imposed by Google or Apple insiders on what counts as acceptable applications of power.

The increasing importance of mobile wireless cellular networks as core Internet infrastructure and these networks' management models are a second control point for us to consider. Wireless carriers have organizational habits rooted in a controlled and optimized network model. The carrier controls what devices are permitted, and knows, manages, and bills all users and usage. Congestion management and quality of service were early initial requirements for these companies, and the use of auctions to allocate spectrum to wireless carriers meant that they saw the physical infrastructure as privately owned and integrated with carriage services. The models of wireless telephony – technical, legal ownership, engineering culture, and business practice – were fundamentally built to enable control by the owner and service provider so as to optimize a known set of services to known paying consumers. These characteristics stood in contrast to the Internet model, through which carriers were legally excluded from control over the network; users and usage were unknown and assumed unknowable; resilient best-efforts, not quality of service, were the core commitment; flexibility to unknown, new uses and users trumped optimization for known uses and users; and any network and open-standards-compliant device could be connected to the network on an equal basis.

The most obvious example of power that follows directly from the historical model of wireless telephony was AT&T's requirement that Apple prevent Skype from using cellular (as opposed to WiFi) data on the

iPhone. Similarly, when carriers impose data caps, but then exclude favored services from counting against those data caps, they nudge users to adopt the preferred applications. In both cases, ownership of the spectrum and the service, the concept of optimization, and the integration of use with known paying users permit the company to exert control over what users can do and what companies unaffiliated with the service providers can offer. The controlled infrastructure, even where built to support control by commercial providers, also facilitates greater control by government agencies. The NSA's collection of bulk metadata from U.S. phone providers offers an obvious example of the more systemic shift in power that this new, more centralized architecture enables.

Packet discrimination and the end of legacy telephone copper-wire as physical infrastructure for broadband form a third control point. The first generation of Internet access by the public took place over dial-up connections. Becoming an ISP required little more than a modem bank connected to a phone line for users to dial; providers numbered in the thousands. The move to cable broadband and DSL over telephone lines increased the complexity of providing service and reduced the number of potential competitors. The deployment of the cable broadband DOCSIS 3.0 standard after 2006 meant that, in the long term, no more upgrades to the copper-wire telephone infrastructure would do. Only fiber-to-the-home could compete with cable for speed. The substantial civil engineering costs of fiber, in turn, reintroduced natural monopoly economics into home broadband markets, making competition a relatively weaker source of discipline for providers.[5]

The practical implication of the death of copper was that the home broadband provider became a significant point of control. At no point was this clearer than in the net neutrality debates. Most prominently, from late 2013 to early 2014, Netflix, Comcast, and Verizon FiOS clashed over whether the carriers were slowing Netflix's service in order to extract payment for adequate service. Independent studies confirmed that the slowdown occurred at the peering point – where Cogent and Level 3, carriers that Netflix uses to carry its traffic, connected to the Comcast and Verizon networks – and was likely caused by business disputes, not technical issues.[6] The parties blamed each other; but for our understanding, the vital development is that the gateway to the home broadband connection has become a central point of control, over which large corporations struggle (to the detriment of both end-users and competitors in the cloud who are not party to negotiations).

The re-emergence of natural monopoly economics in home broadband leaves us with a market or regulatory design choice, not a technical design choice. Barriers to entry into the wired home broadband market will continue to be high in the foreseeable future, hampering the efficacy of market solutions. Regulation in a number of forms seems most likely to diffuse power; this will likely require a combination of utility regulation – interconnection and interoperability on nondiscriminatory terms – and net neutrality rules requiring nondiscrimination among applications and content.

The emergence of cloud computing – enabled by increased speed of communications and widespread adoption of mobile computing – forms a third vital control point. Increasingly, individuals and businesses run their computation and storage remotely, on large computing and storage clusters owned and managed by third-party providers. This shift allows firms to economize on capital expenditures, enhance robustness and security, and scale computation, storage, and applications more flexibly than provisioning their own capacity would permit.

Despite the obvious benefits of cloud computing to individual users and firms, the technology also has the effect of centralizing power. The now-iconic example is Amazon's decision, in 2009, to delete copies of George Orwell's *1984* and *Animal Farm* from users' Kindles. The company claimed that the books were uploaded to the Kindle Store by a company that did not have the rights to them. Because Kindles are clients to a cloud service that stores and delivers the e-books, Amazon was in a position to delete these unapproved editions unilaterally. The platform, content, and software providers for cloud services all retain technical control over the data and operations of the customer in ways that were simply impossible when data and software were stored locally on the end-user's owned machine. The inherent power concern is not only about what the owner of the cloud provider can do, but also what third parties can do given the concentration of data and software in a single spot. One of the many revelations made by Edward Snowden was that the National Security Agency (NSA) project MUSCULAR had compromised both Google and Yahoo cloud storage facilities to enable the NSA to collect millions of records from e-mails, text, audio, and video from these companies.

What is important here is not that the NSA acted improperly; it is that cloud computing shifted the locus of power. When the data and software of hundreds of millions of people exist or run in a single place, whoever can compromise and gain control over it – legitimately or illegitimately – can exercise power over these hundreds of millions of people, at least to the extent that the data and applications extend power over their users and subjects.

The fourth control point is big data and its uses in behavioral control. In 2014, the *Proceedings of the National Academy of Sciences* reported on an experiment that manipulated the number of positive and negative emotional expressions on users' Facebook news feeds, which correlated with increased expressions by the subjects, of similarly positive and negative emotional content.[7] In sum, people's moods could be altered through manipulation of their news feeds. These findings complemented an earlier Facebook-based study that showed that users who received social messages notifying them that their friends had voted were more likely to vote than users who received no such message, or who received informational messages (as opposed to social).[8] The effect size was small in both cases, but statistically significant. The implication was quickly identified by scholars concerned with the power of Facebook and other companies that both control data and can integrate it, altering the user experience.[9]

Big data collection and processing, combined with ubiquitous sensing and connectivity, create extremely powerful insights on mass populations available to relatively few entities. These insights, together with new computational methods, make up what we think of as "big data." As Zeynep Tufekci has explained, when these methods combine with widespread experimentation (as in the Facebook experiments), behavioral science that analyzes individuals in a stimulus-response framework, and increasingly on-the-fly personalization of platforms, platform companies can nudge users to form beliefs and preferences, follow behaviors, and increase the probability of outcomes with ever-finer precision. These form the foundation of what management scholar Shoshana Zuboff has called "surveillance capitalism."[10] As consumers become more precisely and individually predictable in their behavioral response to experimentally derived stimuli, and platforms become ever-more programmable at an individual level to obtain desired behavioral responses, the idea of individual "preferences" that are exogenous and preexist market relations, and whose satisfaction drives mar-

kets and produces "welfare," becomes incoherent. While the endogeniety of preferences has been a central theme of critiques of markets, at least since economist Thorstein Veblen's *Theory of the Leisure Class*, behavioral manipulation has never been scientifically studied and integrated into service design on such a mass scale as has become possible, and increasingly standard, in big data/surveillance-informed behavioral marketing.

As part of the president's response to the political uproar caused by the Snowden disclosures, the President's Council of Advisors on Science and Technology (PCAST) issued a report on big data. The PCAST report was remarkable in that it repudiated two of the primary approaches we had previously used to preserve privacy: consent and anonymization. Since the emergence of "email privacy" as an issue in the early 1990s, regulatory efforts, particularly in the United States, focused on notice of collection and consent by the data subject. But as the PCAST report put it: "Notice and consent creates a nonlevel playing field in the implicit privacy negotiation between provider and user. The provider offers a complex, take-it-or-leave-it set of terms, while the user, in practice, can allocate only a few seconds to evaluating the offer. This is a kind of market failure."[11] As for anonymization, PCAST found that "[a]nonymization is increasingly easily defeated by the very techniques that are being developed for many legitimate applications of big data. In general, as the size and diversity of available data grow, the likelihood of being able to re-identify individuals (that is, reassociate their records with their names) grows substantially."[12] Both kinds of obsolescence mark a centralization of power, from individuals to the smaller set of entities capable of setting the terms of standard contracts or collecting, purchasing, and processing sufficient amounts of the ambient data surrounding individuals to defeat efforts at self-protection through anonymization.

PCAST's core recommendation was to accept the futility of regulating data collection and processing and implement more rigorous regulations on uses of collected data. Having diagnosed that both the technical systems involved in anonymization and the market systems involved in consent and contracting cannot alone carry the weight of preserving the *desiderata* we associate with privacy, PCAST shifted the onus of protection to the legal system. But this recommendation is undermined by the fact that the report in which it appears is itself the result of public exposure of a widely perceived failure of legal oversight. The Snowden revelations exposed that the complexity and opacity of the national security establishment rendered legal oversight and control highly imperfect. And this imperfection is not unique to government entities. The literature – ranging from rational-actor modeling through organizational sociology and cognitive bias – tells us that formalized rules imposed externally by a regulatory body are likely to function as imperfectly and incompletely as the technological or contractual subsystems that PCAST rejected. (This could be the case for a number of reasons, whether individual self-interest and agency problems; the force of habits, processes, and routines; or the dynamics of groupthink and bureaucratic culture.) All of these systems are radically incomplete and flawed, and it will be exceedingly difficult for any one of them to carry the burden of reversing a power flow instantiated in the basic architecture of the interaction.

The Netflix effect, and the increased identification of content as culture, form the final new control point I will discuss here. In January 2014, author and activist Cory Doctorow wrote a short post on his website, "We Are Huxleying Ourselves Into the Full Orwell." Doctorow was commenting on

the possibility that the W3C would adopt a standard for HTML5 that implements Digital Rights Management (DRM) in the basic browser standard.[13] The W3C was then being pushed to do this by browser manufacturers Microsoft, Apple, and Google, who were, in turn, being pushed by Netflix, which demanded DRM to assure its capacity to prevent users from creating unauthorized copies of its licensed content. By May 2014, not only had the W3C adopted the DRM standard, but the Mozilla Foundation, developer of the leading FOSS browser, had bowed to the perceived necessity of enabling users to view Netflix and released its own implementation of the DRM standard for HTML5. Together, these events reflect both the shift in cultural power and erosion of one of the core institutional and organizational mechanisms that made the Internet a force for decentralization of social, economic, and cultural power.

These events implicate several of the core design features of the early Internet and the policy battles to make it more readily susceptible to control. First, DRM technologies are a perfect example of an effort to impose power through technology. The essence of these technical measures is to allow one entity, originally a copyright owner, to determine who may make what uses of digital objects protected by DRM. The point is not legitimacy or legality, but power. DRM may be used equally to prevent unauthorized copying or to prevent legitimate fair uses of, or permissible innovation with, the encrypted materials. DRM technologies are designed to remove practical capacity to make a judgment about the legitimacy of a use from the possessor of the materials, and to locate that power with the copyright owner.

Although the U.S. Congress passed the Digital Millennium Copyright Act (DMCA) in 1998, which prohibited DRM circumvention, circumvention practices and devices have been trivially available to anyone who has chosen to use them. The practical capacity of copyright holders to control circumvention was nonexistent for music, and marginal for video. The adoption of DRM for video streaming as part of HTML5 sees the Web, one of the core open standards underlying a major use of the Internet, embed the control mechanism within it. The process of doing so exemplified an increasing role for major companies in the governance of standards, which had previously been more anarchic. Moreover, the adoption occurred due to widespread consumption patterns that put the Mozilla Foundation, a nonprofit organization dedicated to coordinate a FOSS project, in the position of either implementing a version of DRM or losing user share and becoming marginalized. It therefore suggests that the shift to widespread passive consumption usage patterns weakens the role that FOSS development could play to provision a separate, power-diffusing alternative infrastructure. The result is not only the singular decision to implement a particular technology; it is diagnostic of basic pressures created when the Internet intersects with mass media culture.

If commercial video is so important, what can we make of the claimed democratizing effect of Internet culture? Nielsen surveys suggest that watching video on the Internet represents about one-third of the amount of personal computer Internet use time for eighteen- to thirty-four-year-olds, about one-quarter for thirty-five- to forty-nine-year-olds, and about 15 percent for fifty- to sixty-four-year-olds.[14] Video on smartphones represented a smaller category of use. Imperfect measures, such as the relatively large share of Internet bandwidth consumed by Netflix in North America (about 35 percent),[15] and the high and growing rates of Netflix subscriptions among North American Internet users (rising from 31 percent to 38 percent of U.S. consumers from 2012 to 2013)[16] reflect the growing

significance of passive watching of professionally produced video entertainment online. Perhaps we are observing a shift toward using the Internet in ways more reminiscent of mass media than of the more culturally decentralized manner celebrated in the middle of the last decade, when fan videos and remixes were all the rage. Data from the Pew Research Center have suggested otherwise.[17] The proportion of adult American Internet users who have uploaded videos more than doubled from 2009 to 2013, reaching about one-third of Internet users. About 18 percent of users uploaded videos they produced for others to watch. Almost three-quarters of American adults online watch videos on YouTube, with comedy (57 percent), "how-to" (57 percent), educational (50 percent), and music videos (50 percent) being the most commonly viewed. These statistics suggest that while Internet users indeed seek Netflix and similar subscription services extensively, they also seek online video rooted in user-created, fan-shared videos. Importantly, the proportions of copyright-connected practices (comedy and music videos) and educational and free knowledge exchange ("how-to") videos are roughly similar.

From the perspective of cultural power, the rise of Netflix does not seem to imply displacement of distributed creativity. Rather, it occurs alongside continued expansion of decentralized cultural creation and decentralization of power, which can encourage, for instance, inserting memes and new frameworks into cultural discourse. Commercial platforms, like YouTube, Vimeo, and Flickr, developed to facilitate creation and distribution of culture by diverse users, offer one important pathway through controlled frameworks – like the app store on the handheld device – for continued sources of cultural decentralization to persist online. Nonetheless, the rise of proprietary video streaming as a major application seems to have been enough both to put pressure on the standards-setting process and to push a major actor in the FOSS development world to abandon a twenty-year-old battle against implementing DRM in the basic standards of core network platforms. Consumption choices appear to severely constrain the freedom of action of public-facing software development FOSS projects; interventions, if any, must be at the level of shaping demand, on the model of ethical or environmentally conscious consumption campaigns, rather than focusing solely on ethical design.

From the early days of public adoption of the Internet, there have been those who have seen decentralization primarily as a threat, empowering the nefarious, from criminals and pirates to pedophiles and terrorists to run-of-the-mill trolls and spammers. But because adaptive, flexible, loosely coupled systems were more likely to improve innovation and resilience in the face of rapid change and high uncertainty than controlled, optimized, well-behaved systems, the original Internet's design reflected a sensibility that treated stasis as far more detrimental than disruption. Unless one is willing to claim that, on balance, that assumption was wrong for the past thirty-two years, that the next thirty-two years are likely to be less rapidly changing and uncertain, or that the risks that agility and rapid innovation present vastly and reliably outweigh their benefits, it seems that the Internet's original design sensibility should continue to guide our future design choices. While defending that commitment is beyond the scope of this essay, I here outline a set of design interventions and challenges implied by present concentration trends, for those who wish to preserve the decentralizing effects of the early Internet.

Major companies and the state are the primary loci of centralizing power in contemporary society. One of the core lessons of the Internet has been that with the ap-

propriate platforms, individuals acting in peer networks can cooperate effectively without relying on the state or the market. In doing so, they create their own (however imperfect) alternative platforms for interaction, which, in turn, impose different constraints than do state-based or market-based organizations. That diversity of constraint (rather than an unattainable absence of power) allows individuals to bob and weave between different efforts – from diverse sources – to impose power on them. This both diffuses some of the centralized power and creates avenues for decentralized power.

User-owned and commons-based infrastructure are one major space of intervention. Perhaps the clearest design targets are the emerging wireless networks necessary to ubiquitous computing, including both handheld networks and the Internet of Things. For many years, proprietary spectrum allocations owned by wireless carriers – coupled with proprietary cell towers – were deemed necessary for mobile computing. It has now become clear, to the contrary, that unlicensed wireless allocations (spectrum commons) running over small-cell networks, owned by diverse organizations and individuals, are likely to be the infrastructure of first and last resort for data, with large-cell proprietary spectrum networks offering the backup for highly mobile, latency-sensitive communications.[18] The main challenge to leveraging this fact into a decentralization of power over wireless networks is to design technical and contractual systems that can permit unrelated individuals to share access to their diversely owned wireless spots. With the exception of relatively few community networks, most widespread WiFi networks are operated by companies like BT Group's system in the United Kingdom or Comcast's emerging model in the United States. Nothing technical prevents these companies' consumers from sharing their access with each other without the carrier. The constraints, instead, are contracts and social habits. One of the core design targets of any future effort to keep the Internet open, decentralized, and resistant to control is to develop technically instantiated mechanisms to achieve user-owned and -shared capacity that offers no proprietary point of control for centralizing actors.

What is true of wireless also holds for cloud storage and computing resources, though it may be more difficult to implement. Past efforts to develop distributed storage or computing include computer scientist Ian Clarke's Freenet, an early peer-to-peer data storage and communications network focused on assuring a secure system for dissidents. Oceanstore, a storage utility built atop an infrastructure of servers, and developed at the University of California, Berkeley, was a later development. Freedombox is an aspirational plug-server architecture proposed to create secure, user-owned servers that would offer much of the robustness and temporary scaling of servers provided by corporate actors, without the centralization of power. These efforts outline a critical area of open infrastructure innovation necessary to counter the centralization effects of cloud storage.

Another major design question concerns open defaults. In the case of the Android app stores explored above, Android OS phones' default settings do not permit sideloading. In WiFi devices, closed, encrypted networks are the default setting. Even though these defaults can be overridden by the user, long-term experience suggests that defaults stick. A critical target of consumer advocacy needs to be for firms that sell infrastructure and basic tools to ship them with open and secure defaults, so that user choice becomes the easy default option.

Open standards, FOSS, and law in the handheld and app-store space must also be directed to open these major control points. Deconcentrating power around the hand-

held and the app store suggest, first and foremost, efforts to develop alternatives through Web-based standards. HTML5 created the possibility of creating the look and feel of an app using an open-Web interface that need not be downloaded from an app store. As of 2015, substantial numbers of developers use HTML5 for its capacity to run across platforms, and its independence from platform-specific training and knowledge. But at this stage, it appears to sacrifice performance and optimization for generality. As long as this is true, and the rate of improvement in handheld operating systems is high, it seems unlikely that the general Web standards–based application development environment will outpace native application development. The power of the app store will remain.

An alternative would be the development of a FOSS handheld operating system (OS), such as the OS that the Mozilla Foundation is developing. As in the case of the Firefox browser, the presence of a FOSS alternative, with a strong institutional basis incorporated as a foundation dedicated to keeping the platform open, can play a role in preserving an open, decentralizing Internet. However, as the earlier discussion of DRM clarifies, that affordance is not an absolute bulwark against centralization; it is, nonetheless, a pathway to preventing additional concentration of power around the app store. If both pathways fail, it is possible that app stores will reach a point when they exercise so much control over effective access to a majority of Internet users that a legal intervention will be necessary to require app-store owners to adopt some form of nondiscrimination policy. Legal action may also be necessary to change defaults so that an app developer can initiate including itself in the app store, and the owner can only constrain access under well-specified, harm-prevention terms.

The adoption of strong, user-controlled encryption by default is one design intervention that seems both feasible and, on balance, justified. By "user-controlled," I mean encryption that provides affordances to the owner of the device on which the encryption is implemented, and constrains action on that device by others. This is by contradistinction from DRM software, which also involves end-device encryption but treats the device owner as the potential attacker, and permits some external third party (such as the copyright owner or the employer of the device owner) to use the encryption to control both uses of and access to the device. Universal strong encryption protects against both centralizing forces – primarily states and companies other than those with which the user has contracts – and decentralized sources of power, such as black hat hackers (crackers), thieves, and terrorists.

The primary opposition to adoption of universal strong encryption comes from those who suggest that the risks associated with technologically supported decentralization outweigh its benefits, and that the risks of centralization can be counterbalanced by institutional constraints on the centralizing power more flexibly and accurately than by technical barriers managed by users. The primary position of major governments is that bodies like the FBI or the NSA, properly constrained by legal oversight, will do far more good than harm if they can access any communication or device. The basic problem with this argument is that it assumes both the effectiveness of the government agencies responsible for order, and the effectiveness of the institutional controls.

As the Internet of Things blossoms, the sheer magnitude of data flows and potential points of attack becomes overwhelming to any system that seeks to read all networked information, predict events based on this data, and interdict those events. By contrast, the possibility of protecting targets locally at the individual-device level

substantially increases the cost and difficulty of harming devices and the data they store, or the processes they control. Defense will be largely imperfect, particularly against a determined and focused attack, but abuse will be more contained than with a universally less-secure system.

Moreover, the assumption that abuses by governments or companies can be adequately constrained by institutional and organizational processes is questionable at best. First, it applies, at most, to democracies with robust rule of law. For billions of Internet users in countries with weak or no rule of law, ubiquitously available strong encryption is the sole defense against abuses. Second, in democratic countries, the fifteen years since September 11, 2001, have seen persistent, repeated, and pervasive violations of human and civil rights and a persistent reluctance by authorities and courts to redress government excesses and mistakes. Multinational companies, in turn, often use jurisdictional arbitrage to escape regulation legally. The fact of the matter is that institutional systems are highly imperfect, no less so than technological systems, and only a combination of the two is likely to address the vulnerability of individuals to the diverse sources of power and coercion they face.

Future design must also take into account the resilience, redundancy, and diversity of systems resources and pathways. A central lesson of the original Internet design – its successes and failures – is that perfection is a fool's errand. Complexity is a basic condition of a connected, dynamic, open society, and with it comes persistent uncertainty and imperfection. Just as the original Internet design rejected perfectibility and optimization for openness, loose-coupling, and continuous experimentation, learning, and adaptation; so, too, must the future Internet. Any effort to finely design the environment so that it will generally permit legitimate power to flow in the legitimate direction, but constrain illegitimate power, will fail often and, sometimes, spectacularly. We need systems that are resilient, robust, and rich in redundant pathways that are open to users to achieve any given range of goals they adopt for themselves. Freedom from power, in this context, inheres in diversity of constraint; and freedom of action is maintained by bobbing and weaving between diverse efforts to impose power on the individual, rather than by following prescribed paths, such as asserting one's rights through proper channels or living on a mountaintop. The practical implication of this rather abstract statement is a simple one: design efforts need to resist calls for optimization and greater control by trusted parties if these come at the expense of open, redundant pathways and resilient capabilities.

One way of constraining power in various arenas is to create mechanisms for assuring distributed audit and accountability, rather than permission. We have auditors in government bodies and require independent auditors to certify company books; the rising call for police officers to wear body cameras so as to deter police abuse and enable redress are also (highly contested) examples of technologically instantiated audit and accountability systems. So, too, could one imagine building an effective audit and accountability system into the Internet design to enable identification and accountability of abusive power. A major concern with any such system is that it would itself create a point of centralization: in the hands of whoever controls the audit trails, or breaks into them.

It is also possible that approaches based on the blockchain could provide a useful space for developing automated audit trails. Blockchain, the technology underlying the cryptocurrency Bitcoin, is still in its infancy. But the core design characteristic may outline a solution for distributed audit trails and accountability that would avoid the

risks of reconcentration. At its core, the technology consists of three components. The first is a ledger that records all assets and transactions in a given domain. The second is encryption, which protects this ledger from tampering. And the third is distributed, redundant storage with mutual accountability such that tampering anywhere becomes evident unless it can be achieved everywhere simultaneously. This outlines an open system that would nonetheless withstand many attacks (both official and unofficial) and provide distributed users with a higher degree of confidence that abuse can be traced, documented, and ultimately fed into a system of accountability than might be possible with a more centralized and institutionalized audit system. Of course, real world accountability will require institutional and organizational adaptations; an automated audit system, decentralized or otherwise, will not be self-executing. But building an audit system with a distributed, robust architecture may offer a technical foundation around which institutions can develop.

A final proposed space for design intervention is user-owned and/or ethical governance in platforms. One of the most remarkable features of the early Internet was the emergence of working anarchies as functioning organizations with substantial social and economic impact. The IETF was the clearest example, in which an organization with practically no recognized order, functioning on self-organized, distributed, discursive arrangements independent of market, state, or other well-behaved sources of accreditation or empowerment, came to manage the core piece of global infrastructure of the late twentieth century. FOSS projects and Wikipedia followed, as the idea of self-motivated action and effective, collective work in self-governing communities matured and came to fulfill a significant part of our core utilities in networked society and economy. As these organizations matured, they began to develop hybrid approaches, mixing formal nonprofit incorporation with internal meritocratic, nonhierarchical structures (such as the W3C, the Apache Foundation, and the Mozilla Foundation), or independent community structures, alongside and of superior legitimate power than the formal foundation set up alongside them (Wikimedia Foundation and the Wikipedia community). As we look ahead toward the design of the future Internet, many challenges will appear to require structured organizational responses, like state-based agency intervention or market-based, proprietary companies. What the past twenty years of self-organized communities suggest is that peer production and social self-organization offer a diverse and rich design space for solving collective action problems and implementing organizational effectiveness without necessarily falling into the trap of state or market, and without simply permitting the emergence of unaccountable oligarchies instead.

When the Internet was first designed, few knew about it, and fewer understood its significance. The major design decisions were made in a power vacuum. By now, everyone knows that Internet-design decisions will affect political, economic, institutional, social, and cultural arrangements, and decisions that will influence the next quarter-century are all being influenced themselves by sustained efforts of diverse parties that stand to benefit from them.

Much virtual ink has been spilled on democracy, innovation, privacy, and cyberhacking, which all address the fundamental problem of power. In all these more familiar framings, how the Internet enables or disables some people to influence the perceptions, beliefs, and behaviors, as well as the outcomes and configurations that other people hold and inhabit, is at stake. In the second half of the twentieth centu-

ry, core values of individual autonomy and self-authorship, creativity and ingenuity, community cooperation, and collective self-governance were all associated with representative democracy; civil rights; the rule of law in property, contracts, and the state; coordination through prices in markets; and stable social institutions, like the family, church, union, and civic association. In the past quarter-century, looser associations have become effective, while these more traditional institutions continued to offer some degrees of freedom and effective action, but also became sources of constraint vis-a-vis the new forms of action and association.

As we struggle with diverse design choices, it is important to recognize the substantial emancipatory and creative power of the open and loosely coupled action systems that the early Internet enabled and empowered. Their force in supporting creativity, autonomy, and chosen association is often linked with relatively weaker governability and less-focused capacity to express a coherent voice. While we have had examples of successful collective action by distributed, Internet-enabled forces over the past few years, the steady grind of policy-making and standards-setting mean that the values of a genuinely open Internet that diffuses and decentralizes power are often underrepresented where the future of power is designed and implemented. Thus, it falls to those primarily in the relatively independent domain of academia to pursue these values and insist on diagnosing design choices in terms of their effects on the distribution of power, as well as to develop and advocate design options that will preserve the possibility of decentralized, autonomous, and organically chosen collective action. Our alternative would be transmitting the power of those organizations that have the wherewithal to sit at every table, and in every conference room, to assure their own interests in the design of our future.

ENDNOTES

1 Tyler Lopez, "How Did Ukraine's Government Text Threats to Kiev's EuroMaidan Protesters?" *Slate*, January 24, 2014, http://www.slate.com/blogs/future_tense/2014/01/24/ukraine_texting_euromaidan_protesters_kiev_demonstrators_receive_threats.html.

2 David Clark, "A Cloudy Crystal Ball – Visions of the Future," in *Proceedings of the Twenty-Fourth Internet Engineering Task Force*, ed. Megan Davies, Cynthia Clark, and Debra Legare (Cambridge: Massachusetts Institute of Technology, 1992), 539 – 545, http://ietf.org/proceedings/prior29/IETF24.pdf.

3 comScore, "The U.S. Mobile App Report," (Reston, Va: comScore, 2014), http://cra.org/wp-content/uploads/2015/02/The-US-Mobile-App-Report.pdf.

4 Jonathan Zittrain, *The Future of the Internet and How to Stop It* (New Haven, Conn.: Yale University Press, 2008).

5 Jon Brodkin, "Netflix Performance on Verizon and Comcast Has Been Dropping for Months," Ars Technica, February 10, 2014, http://arstechnica.com/information-technology/2014/02/netflix-performance-on-verizon-and-comcast-has-been-dropping-for-months/.

6 Measurement Lab Consortium, *ISP Interconnection and Its Impact on Consumer Internet Performance*, October 28, 2014, http://www.measurementlab.net/static/observatory/M-Lab_Interconnection_Study_US.pdf; and MIT Information Policy Project, in collaboration with the UCSD Cooperative Association for Internet Data Analysis, *Measuring Internet Congestion, A Preliminary Report* (Cambridge: Massachusetts Institute of Technology, 2014), https://ipp.mit.edu/sites/default/files/documents/Congestion-handout-final.pdf.

7 Adam D. I. Kramer, Jamie E. Guillory, and Jeffrey T. Hancock, "Experimental Evidence of Massive-Scale Emotional Contagion Through Social Networks," *Proceedings of the National Academy of Sciences* 111 (29) (2014): 8788 – 8790.

8 Robert M. Bond, Christopher J. Fariss, Jason J. Jones, et al., "A 61-Million-Person Experiment in Social Influence and Political Mobilization," *Nature* 489 (7415) (2012): 295 – 298.

9 Zeynep Tufekci, "Engineering the Public: Big Data, Surveillance, and Computational Politics," *First Monday* 19 (7) (2014), http://firstmonday.org/ojs/index.php/fm/article/view/4901/4097; and Jonathan Zittrain, "Facebook Could Decide an Election Without Anyone Ever Finding Out," *The New Republic*, June 1, 2014, http://www.newrepublic.com/article/117878/information-fiduciary-solution-facebook-digital-gerrymandering.

10 Shoshana Zuboff, "Big Other: Surveillance Capitalism and the Prospects of Information Civilization," *Journal of Information Technology* 30 (1) (2015): 775 – 789.

11 President's Council of Advisors on Science and Technology, *Big Data and Privacy: A Technological Perspective*, (Washington, D.C.: Executive Office of the President, May 2014), xii, https://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf.

12 Ibid., xi.

13 Cory Doctorow, "We Are Huxleying Ourselves Into the Full Orwell," Mostly Signs, Some Portents, January 9, 2014, http://mostlysignssomeportents.tumblr.com/post/72759474218/we-are-huxleying-ourselves-into-the-full-orwell.

14 Proportions calculated by author from Nielsen, *The Total Audience Report* (New York: Nielsen Company, December 2014), http://www.nielsen.com/content/dam/corporate/us/en/reports-downloads/2014%20Reports/total-audience-report-december-2014.pdf.

15 See Sandvine, *Global Internet Phenomena: Asia-Pacific & Europe* (Waterloo, Ontario: Sandvine Incorporated, 2015) as discussed in Adam Epstein, "Netflix Now Accounts for 35% of Bandwidth in the U.S. and Canada," *Quartz*, November 20, 2014, http://qz.com/299989/netflix-now-accounts-for-35-of-bandwidth-usage-in-the-us-and-canada/.

16 Nielsen, *The Digital Consumer* (New York, The Nielsen Company, February 2014), http://www.nielsen.com/content/dam/corporate/us/en/reports-downloads/2014%20Reports/the-digital-consumer-report-feb-2014.pdf.

17 Kristen Purcell, "Online Video 2013" (Washington, D.C.: Pew Research Center, October 10, 2013), http://www.pewinternet.org/2013/10/10/online-video-2013/

18 President's Council of Advisors on Science and Technology, *Big Data and Privacy: A Technological Perspective*; and Yochai Benkler, "Open Wireless vs. Licensed Spectrum: Evidence from Market Adoption," *Harvard Journal of Law & Technology* 26 (1) (2012): 69 – 163.