INTRODUCTION

Robert Faris & Rebekah Heacock

Each day, the choices and policies that shape the contours and impact of the Internet become more consequential. An increasing proportion of economic, social, political, and cultural events and struggles are played out in the digital realm, either exclusively in virtual form or in conjunction with offline events. The power dynamics of the Internet are becoming increasingly indistinguishable and inseparable from the wider world.

In digital spaces, we see governments continue to grapple with different approaches to the regulation of digital activity. Some governments aspire to limit the impact of regulation on innovation and protected speech while others resolutely curtail freedom of speech and assembly. We see companies seek to attract and manage customer bases while balancing the contradictory demands of regulators and users. Meanwhile, individuals and civil society groups leverage the affordances of digital technologies to shape political and social outcomes—in some cases with the support and protection of governments and companies, and in others working around the constraints governments and companies impose upon them.

> ***We're in the midst of an epic battle for cyberspace.... We need to decide on the proper balance between institutional and decentralized power, and how to build tools that enable what is good in each while blocking the bad.***
>
> —BRUCE SCHNEIER
> Power in the Age of the Feudal Internet

One of the key themes that emerge from the collection of essays in this publication is the contest to redefine power relationships in digital spaces among governments, companies, and civil society, and the very different ways in which this struggle is manifest in different societies and countries around the world. The power of civil society is strengthened through higher levels of connectivity, unfettered access to knowledge, freedom of expression, and freedom to engage in collective action facilitated by digital tools: in short, the creation of social capital online. For governments, the quest for power tends to focus on establishing the legal means and mechanisms to uphold laws in the digital arena but also extends to encouraging and sustaining an environment that is conducive to innovation and collaboration. The calculus for companies is on one hand very straight-forward—being able to engage in profitable commercial activity—and on the other hand highly complex, as they occupy the difficult space between the conflicting demands of governments and citizens.

A legacy of prior architectural and policy choices frame and constrain the current state of play. Lessig's framework of four forces that interact to regulate Internet activity—architecture, markets, laws, and social norms—is as apt today as it was when published fifteen years ago, perhaps several generations of digital time. Code is still law, though expressed in many unforeseen ways by the platforms and applications that attract so much of our digital transactions. Market activity has rapidly seized opportunities that have arisen, and the architecture of the Internet, encompassing both physical and software, strongly follows the contours shaped by market forces. Social norms continue

to evolve in fits and starts, via compromises and conflicts. And formal legal structures, moving at the measured speed of their governmental deliberation and process—although seen by many as advancing too quickly and too aggressively—seek to regain jurisdiction in areas of real and perceived lost sovereignty. The laws that have acted to protect expression—for example, limits on intermediary liability—have had a profound impact. Others that seek to reign in expression have not met the same success, in some cases far exceeding the targets of regulation while often failing to address the ills for which they were intended. Still others have failed in the presence of technological end runs and popular opposition. Of the power voids that characterized the early day of the Internet, fewer and fewer remain.

While the Internet was once seen as a separate realm populated by independent-minded pioneers that would collectively create the rules and norms of this new landscape, the current and future struggles over control of the Internet are now dominated by large players, primarily governments and large companies. For individuals, this means navigating a tricky and at times treacherous online landscape. In many cases, governments act in their interests, helping to provide the connectivity and skills to take advantage of digital opportunities, protecting civil liberties while deterring malicious actors. In other cases, governments act as obstacles, via inappropriate regulations, repression, and invasive surveillance. Similarly, companies that provide the infrastructure, services, and applications that facilitate digital expression and community formation are alternately seen as allies and adversaries.

In many respects, the distributed and decentralized vision of the Internet has persisted, for example, in the ways that individuals can offer opinions and form multiple interrelated networks of friends and colleagues, and in the cooperative and collaborative forms of cultural production that have emerged. In other important ways, the Internet is highly centralized and hierarchical. A modest number of Internet service providers act as gateways to the Internet for a large majority of people. A handful of companies—Baidu, Google, Sina, Facebook, Twitter and others—dominate search, social media, and social networking online. These overlapping and contradictory structural features mirror the ongoing struggle for control over the limits to online speech and access to personal information.

None of this goes unwatched. The promise and scourge of the Internet is that it is highly reflective, and with each passing day the Internet offers a clearer window into society. Those with the means to capture the digital traces and reassemble the constituent parts can uncover more and more of the relationships, ideas, and sentiments of those that inhabit virtual spaces. Arguably, the individual and collective information offered through digital communication reflects an unparalleled view of the underlying world—one that is more accurate and more representative than any of the alternatives of the past and one that is slowly converging on a comprehensive picture of the communities and institutions that vie for power and influence in societies across the globe. In places, this convergence of online and offline arenas is readily apparent. For much of the world, it has scarcely begun.

Although still fragmented and fractured, the emergence of this detailed, information-rich view of the world represents both the power and the bane of digital expression. This granular view of personal thoughts and activities is in many ways too intimate. The distinction between public and private has blurred in digital spaces to the detriment of personal privacy and the prior negotiated boundaries between private communication and government access to personal data. This profusion of personal data has many benefits that are more evident by the day, spurring research and innovation in health,

education, industry, transportation, and planning, along with innumerable economic applications. The often-repeated mantra appears to be generally true: digital tools can be a powerful means for broader swaths of society to influence the public agenda and for civil society interest groups to mobilize like-minded people for social and political causes.

None of this suggests that there are any inevitable outcomes, only that any dreams of a cyberspace defined primarily by autonomous individuals are receding into the distance. The Internet is at the same time both freeing and feudal. The essays collected here highlight the several and distinct fault lines that mark the ongoing policy debates and power struggles.

Expanding physical infrastructure, penetration and use

Internet penetration—the percentage of people using the Internet—worldwide has been steadily rising, and reached 41.8 percent of the global population, or around 2.9 billion people, last year. Major obstacles to access, including cost and lack of infrastructure, remain in many parts of the world. Monthly wireline broadband subscription charges in low income countries are nearly three times as expensive as in high income countries; penetration rates in high income countries are nearly five times as high as those in low income countries.[1] These divides are apparent regionally as well: Sub-Saharan Africa's penetration rate is less than one third that of either Latin America or the Middle East and North Africa, and less than one seventh that of North America.

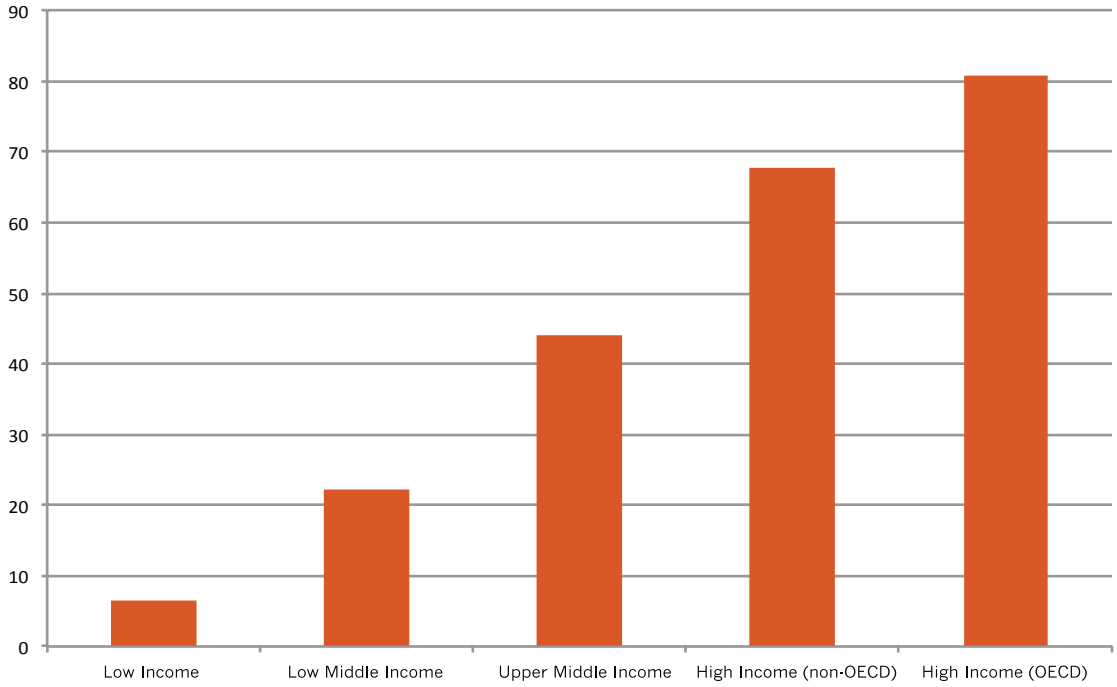

Figure 1: Percentage of individuals using the Internet (2012), by national income level

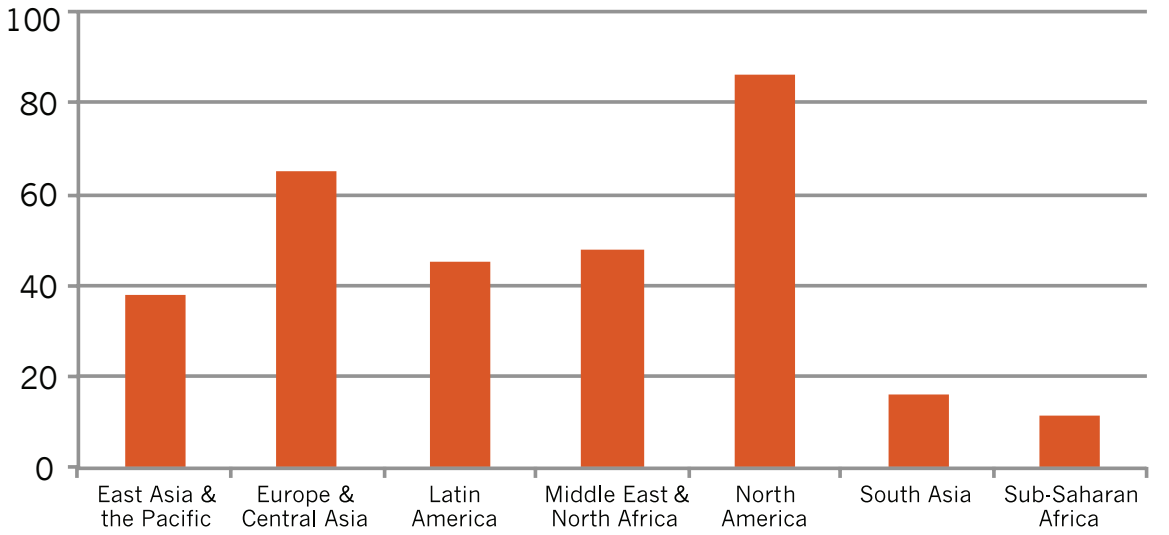

Figure 2: Percentage of individuals using the Internet (2012), by region

Mobile subscriptions continue to see rapid growth, with the average global mobile subscription rate crossing the 100 percent line for the first time in 2012. Growth is particularly rapid in low income countries, with the mobile subscription rate rising by 14 percent from 2011-2012, to an average of 70 percent (compared to an Internet penetration rate of just 16 percent). In the vast areas of the world where mobile represents the sole means of connectivity, this leapfrogging may be a mixed bag: mobile connectivity is better than nothing, but may be an inferior substitute for high-speed wireline broadband access.

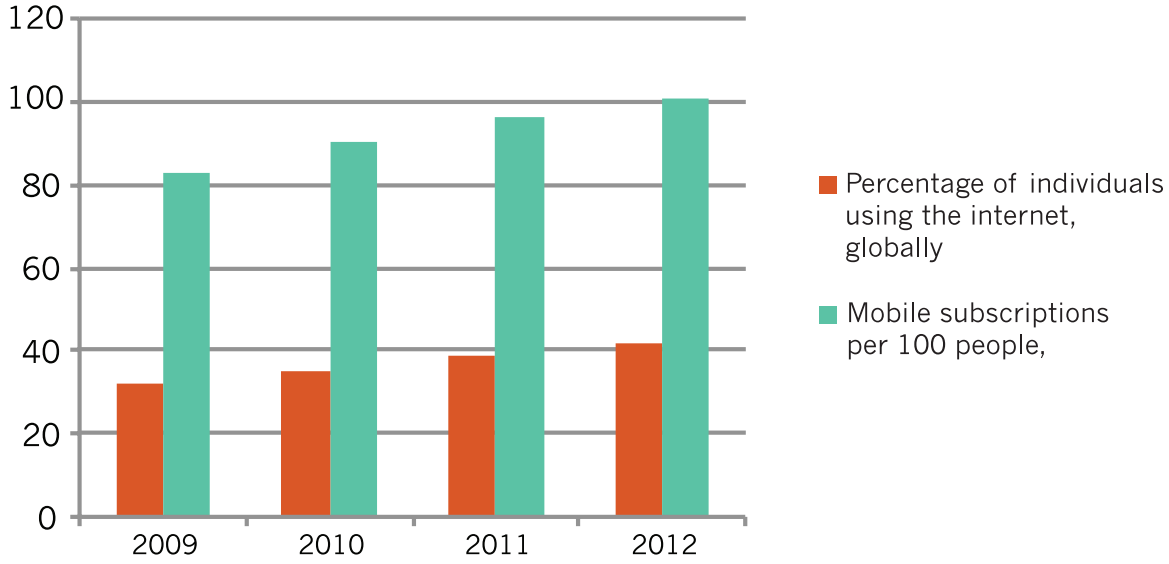

Figure 3: Mobile subscription rate vs. Internet penetration rate, global average

In the past year, a number of major industry players, including Google (through Project Loon) and Facebook (partnering with a range of mobile technology companies through Internet.org), have announced initiatives to increase Internet access in underserved areas. These projects join a number of other efforts in exploring the possibilities of new technologies such as wireless broadband, coupled

with policies aimed at promoting competition and innovation in the space, to bring affordable, quality Internet access to the remaining three-fifths of the world's population.

Trends and points of contention

A number of trends and themes arise in the essays compiled here that shape the evolving balance and distribution of power among governments, companies, and civil society as they vie for influence and control. At the core are questions about who can contribute, in what manner, and who has access to what information.

The trends we describe here are not sudden shifts but the cumulative result of changes that have been underway for many years, each of which has been reinforced over the past year. These issues are all intimately related to one another and reappear frequently in the essays included in this publication.

We are forced to recognize that state surveillance touches all aspects of Internet life, affecting not only the ability of states to assert control in digital spaces but also security, privacy, and the formation of functional civil society groups.

The curtain is raised on the surveillance state

It is possible that 2013 will be seen as an inflection point in the history of Internet as citizens, companies, and governments consider the ramifications and responses to digital surveillance. Surveillance colors all aspects of digital activity: not just privacy and law enforcement, but freedom of expression, civil society activity, the structure of markets, future infrastructure investments, and much more.

The biggest story in the digital world over the past year has been the pulling back of the curtain showing the scale and depth of online surveillance carried out by the United States National Security Agency (NSA). Large scale digital surveillance is not new. What is new is the widespread recognition of its existence and its ability to reach into digital corners thought to be out of reach. The large arsenal of hacking tools and apparent broad targeting of tracking activities—tapping into trans-oceanic cables, conducting social network analysis on American citizens, indiscriminate collection of billions of phone records, tampering with encryption standards, and the list goes on—has brought this issue to the forefront of digital security and civil liberties debates around the world.

The NSA may represent the broadest and most technologically advanced surveillance operation in the world, but the US government is not alone in collecting as much information as it is able. A myriad of questions have been raised about the role of surveillance in democratic societies, including the appropriate thresholds that should be in place for collecting and processing private communications, the balance between security and civil liberties, issues of oversight and accountability related to secret programs, the ethics and practical implications of spying on the rest of the world, and the legal status and treatment of leakers. Surveillance practices highlight not only questions about the rights of citizens but also the powerful and uneasy relationship between governments and private companies.

While still far from a popular movement, the calls for reconsidering the social contract that governs

the scope and conditions under which government surveillance takes place both domestically and internationally have increased many fold in the past year, and have the potential to alter the future digital landscape. The debate over individual use of encryption and the right to anonymous speech online is likely to grow.

It will take time to sort out the possible detrimental effects this revelation will have on the global Internet. The responses to this disclosure, which have come from all corners of the globe, may act to reshape the Internet and influence policy decisions for many years to come. A strong reaction came from Brazil, where President Dilma Rousseff announced that Brazil will seek ways to avoid NSA surveillance and reduce its reliance on US-based platforms. Increasing the proportion of traffic to domestically hosted servers and services would bring significant but uncertain implications for Internet users around the world. If successful, a likely outcome would be reduced surveillance by the NSA accompanied by greater access for local governments to user data. This may represent a launching point for increasing Balkanization of the Internet. Other reactions are bound to follow.

Mounting concerns over online privacy

Interest and concern over privacy online continues to attract more attention, though still considerably less than many observers believe is warranted. The revelations associated with the Snowden leaks add to a long list of concerns related to data collection and use by technology companies. There is broad consensus that the traditional modes of privacy protections—informed consent prior to collecting information, restrictions on use and sharing, and stripping identifying information from data releases—are broken, perhaps irreparably so. So far, solutions tailored to the digital age are elusive. Privacy encapsulates multiple complex questions, and individuals differ markedly in how they conceptualize and approach these issues. Yet the notion that people simply don't care is losing credibility.

Cybersecurity questions persist

As the stories of malicious cyberattacks against individuals, companies, and governments continue to mount, attention to Internet security now features prominently in public policy discussions. It is difficult, however, to ascertain whether the risks of conducting business and personal affairs are actually any worse they were than five or ten years ago.

At one level, cybersecurity is almost inseparable from issues of online privacy and surveillance as the lines between watching, collecting, and intrusion into private networks are thin. The mechanisms and tools to protect against cyberattacks overlap in large part with those that are used to maintain privacy and thwart unwanted surveillance. In policy discussions, however, cybersecurity is generally framed in starkly different terms, commonly evoking the language of foreign threats and national interest. A persistent fear among many is that the cure will be worse than the disease: that reactions to cybersecurity will harm innovation and curtail civil liberties online. Along with questions around surveillance and privacy, the issue of cybersecurity highlights the growing challenges for individuals and small entities operating independently on the Internet today.

> ***The second generation [of the networked public sphere] came with the rise of the great global social platforms, Facebook and Twitter.... The hegemony of these giants is the defining feature of NPS 2.0.***
>
> —JOHN KELLY
> Three Generations of the Networked Public Sphere

Big platforms entrenched

The prominent role of a small number of large companies in the digital life of a majority of the world's Internet users is by no means a new phenomenon. It is, however, looking more and more like a permanent fixture of the digital world. Without question, the prominence of big platforms shapes the efficacy of regulatory strategies and the innovative and collaborative potential of cyberspace. It is also inextricably linked to issues of surveillance, privacy, security, and freedom of expression, among others.

Through the cumulative decisions of millions of users and the pull of network effects, a handful of platforms have emerged as both the hosts of a vast amount of private sensitive information and as digital public squares. In the process, and not entirely by choice, they have become extraordinary powerful players in setting regulatory policy online. When governments seek to selectively block content on social media or look for information on users, they turn to Facebook, Google, and Twitter. And when activists campaign for protecting civil liberties online, they focus much of their attention on the same parties.

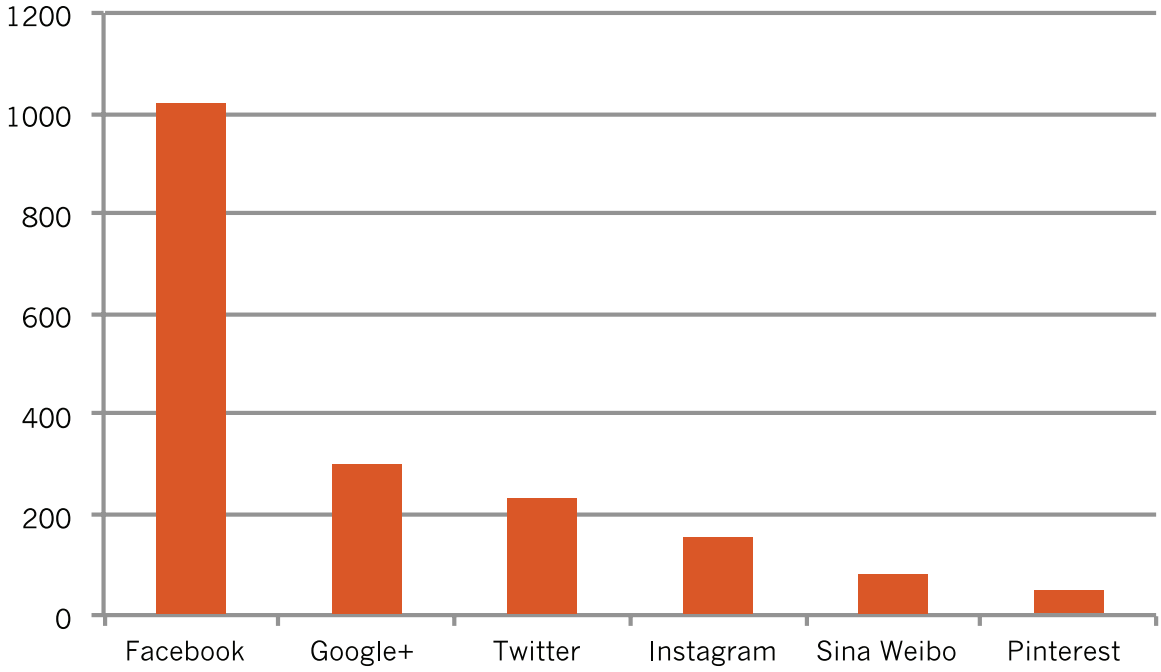

Figure 4: Monthly active users of popular social media sites (in millions)

Large social media companies are now key arbiters of acceptable speech. They make decisions that determine when and how copyright disputes are handled in cyberspace and are asked to act

as watchdogs for human rights and civil liberties online. We are just beginning to learn how much discretion large companies may have in the determining the effectiveness of government surveillance, whether they readily comply with requests for information or push back against such requests. Although not by design, a growing array of important public interests is precariously perched upon a backbone of private infrastructure and market-based decisions.

> ***While youth are not abandoning Facebook, they are now diversifying their time spent on social media by adopting alternative platforms such as Twitter, Instagram, and Snapchat, which invite and support different forms of self-expression.***
>
> —SANDRA CORTESI
> Youth Online: Diversifying Social Media Platforms and Practices

The evolution of network structure in social media suggests that power law distributions could be a natural feature of this landscape, with large social media platforms at the top of the distribution. But it is not obvious that the same major players will continue to occupy the most prominent positions and there are signs that users are seeking out smaller platforms, which suggests that there may be hope still for consumer responses playing a productive role in addressing privacy and security issues.

Regulating digital spaces is not getting any easier

Although different in scale, the core regulatory challenges of the Internet have changed little over the past two decades. If anything, regulating digital speech and information flows is getting more difficult. Digital expression that traverses international boundaries, anonymous speech, the difficulty in attribution, and the massive scale of social media are among the facets that complicate law making in cyberspace. Policymakers around the world continue to draft laws to govern this hard-to-govern medium, with mixed results. Several recent legislative initiatives reveal governments that are intent on reining in Internet speech to more closely align with traditionally stronger offline media regulations: for example, the rumor law in China, Decree 72 in Vietnam, and media licensing requirements in Jordan and Singapore.

As formal regulatory structures are understandably slow to adapt, private ordering has filled this regulatory niche. Standards developed by private platforms to govern activity on their sites have taken on the form of law, guiding and constraining user behavior. At times these standards are in step with the national laws of their users, but more often they are not. When Bing filters the search results for its Arabic language users, or YouTube suspends a user account for the presence of violent material, these privately mediated arrangements play critical regulatory roles, with many of these decisions taking place outside of formal public oversight.

The networked public sphere comes of age (in places)

The list of countries that have been affected by digitally mediated civic action continues to grow. In the past year, protest movements in Turkey and Brazil have occupied headlines. Although many descriptions of "Twitter and Facebook revolutions" over the past several years have been overblown—

suggesting agency to technology tools or proclaiming that technology has decisively changed the pitch of the field in favor of democracy—the role of digital tools in facilitating social mobilization is undeniable.

The roots of these actions can be seen in the opinions and political debates online and in the networks that have formed around ideas and causes. The digital activism and organizing in opposition to new copyright legislation in the United States (SOPA-PIPA), which subsequently spread to Europe to oppose ACTA, was a watershed moment in online organizing. While many may mark these events as the time when the networked public sphere came of age, these examples are still outliers. Across the majority of issues and locations, the networked public sphere remains dormant.

Fighting for alternatives and autonomy

Amid the large companies and governments jostling to mold the Internet in their own interests, a growing number of individuals and smaller entities are fighting to preserve an Internet that more closely resembles the idealized version of a previous generation: an Internet where individuals can act autonomously, exchange ideas freely without fear of government censorship or surveillance, and operate independently of corporate interests. Much of this work is carried out by technologists that develop alternative tools and platforms and activists that seek to stave off legal and political threats to these communities. Frequent allies are found among open government advocates, whistleblowers, and hacktivist groups, and considerable support and sympathy comes from governments and companies. The surveillance revelations of the past year have added much energy and motivation for a strong civil society response to regain lost ground while highlighting the daunting obstacles ahead.

Notes

1. Fixed (wired) monthly broadband subscription charge in 2011 (most recent available data), as reported by the ITU in USD: 98.49 in low and low middle income countries, 35.32 in high income countries (OECD and non-OECD combined). Internet users per 100 people in 2012, as reported by the ITU: 15.9 percent for low and low middle income countries; 74.2 percent for high income countries (OECD and non-OECD combined).

POWER IN AGE OF THE FEUDAL INTERNET

Bruce Schneier

We're in the middle of an epic battle for power in cyberspace. On one side are the nimble, unorganized, distributed powers, such as dissident groups, criminals, and hackers. On the other side are the traditional, organized, institutional powers such as governments and large multinational corporations. During its early days, the Internet gave coordination and efficiency to the powerless. It made them powerful, and seem unbeatable. But now, the more traditional institutional powers are winning, and winning big. How these two fare long-term, and the fate of the majority of us that don't fall into either group, is an open question—and one vitally important to the future of the Internet.

In its early days, there was a lot of talk about the "natural laws of the Internet" and how it would empower the masses, upend traditional power blocks, and spread freedom throughout the world. The international nature of the Internet made a mockery of national laws. Anonymity was easy. Censorship was impossible. Police were clueless about cybercrime. And bigger changes were inevitable. Digital cash would undermine national sovereignty. Citizen journalism would undermine the media, corporate PR, and political parties. Easy copying would destroy the traditional movie and music industries. Web marketing would allow even the smallest companies to compete against corporate giants. It really would be a new world order.

Some of this did come to pass. The entertainment industries have been transformed, and are now more open to outsiders. Broadcast media has changed, and some of the most influential people in the media have come from the blogging world. There are new ways to run elections and organize politically. Facebook and Twitter really did help topple governments.

But that was just one side of the Internet's disruptive character. Today the traditional corporate and government power is ascendant, and more powerful than ever.

On the corporate side, power is consolidating around both vendor-managed user devices and large personal data aggregators. This is a result of two current trends in computing. First, the rise of cloud computing means that we no longer have control of our data. Our email, photos, calendar, address book, messages, and documents are on servers belonging to Google, Apple, Microsoft, Facebook, and so on. And second, the rise of vendor-managed platforms means that we no longer have control of our computing devices. We're increasingly accessing our data using iPhones, iPads, Android phones, Kindles, ChromeBooks, and so on. Even Windows 8 and Apple's Mountain Lion are heading in the direction of less user control.

I have previously called this model of computing feudal. Users pledge our allegiance to more powerful companies who, in turn, promise to protect them from both sysadmin duties and security threats. It's a metaphor that's rich in history and in fiction, and a model that's increasingly permeating computing today.

Feudal security consolidates power in the hands of the few. These companies act in their own self-interest. They use their relationship with us to increase their profits, sometimes at our expense. They act arbitrarily. They make mistakes. They're deliberately changing social norms. Medieval feudalism

gave the lords vast powers over the landless peasants; we're seeing the same thing on the Internet.

It's not all bad, of course. Medieval feudalism was a response to a dangerous world, and depended on hierarchical relationships with obligations in both directions. We, especially those of us who are not technical, like the convenience, redundancy, portability, automation, and shareability of vendor-managed devices. We like cloud backup. We like automatic updates. We like that Facebook just works—from any device, anywhere.

Government power is also increasing on the Internet. Long gone are the days of an Internet without borders; and governments are better able to use the four technologies of social control: surveillance, censorship, propaganda, and use control. There's a growing "cyber sovereignty" movement that totalitarian governments are embracing to give them more control—a change the US opposes because it has substantial control under the current system. And the cyberwar arms race is in full swing, further consolidating government power.

In many cases, the interests of corporate and government power are aligning. Both corporations and governments want ubiquitous surveillance, and the NSA is using Google, Facebook, Verizon, and others to get access to data it couldn't otherwise. The entertainment industry is looking to governments to enforce its antiquated business models. Commercial security equipment from companies like BlueCoat and Sophos is being used by oppressive governments to surveil and censor their citizens. The same facial recognition technology that Disney uses in its theme parks also identifies protesters in China and Occupy Wall Street activists in New York.

What happened? How, in those early Internet years, did we get the future so wrong?

The truth is that technology magnifies power in general, but the rates of adoption are different. The unorganized, the distributed, the marginal, the dissidents, the powerless, the criminal: they can make use of new technologies faster. And when those groups discovered the Internet, suddenly they had power. But when the already powerful big institutions finally figured out how to harness the Internet for their needs, they had more power to magnify. That's the difference: the distributed were more nimble and were quicker to make use of their new power, while the institutional were slower but were able to use their power more effectively.

All isn't lost for distributed power, though. For institutional power the Internet is a change in degree, but for distributed power it's a change of kind. The Internet gives decentralized groups—for the first time —access to coordination. This can be incredibly empowering, as we saw in the SOPA/PIPA debate, Gezi, and Brazil. It can invert power dynamics, even in the presence of surveillance censorship and use control.

There's another more subtle trend, one I discuss in my book Liars and Outliers. If you think of security as an arms race between attackers and defenders, technological advances—firearms, fingerprint identification, lockpicks, the radio—give one side or the other a temporary advantage. But most of the time, a new technology benefits the attackers first.

We saw this in the early days of the Internet. As soon as the Internet started being used for commerce, a new breed of cybercriminal emerged, immediately able to take advantage of the

new technology. It took police a decade to catch up. And we saw it with social media, as political dissidents made quicker use of its organizational powers before totalitarian regimes were able to use it effectively as a surveillance and propaganda tool. The distributed are not hindered by bureaucracy, and sometimes not by laws or ethics. They can evolve faster.

This delay is what I call a "security gap." It's greater when there's more technology, and in times of rapid technological change. And since our world is one in which there's more technology than ever before, and a greater rate of technological change than ever before, we should expect to see a greater security gap than ever before.

It's quick vs. strong. To return to medieval metaphors, you can think of a nimble distributed power—whether marginal, dissident, or criminal—as Robin Hood. And you can think of ponderous institutional power—both government and corporate—as the Sheriff of Nottingham.

So who wins? Which type of power dominates in the coming decades?

Right now, it looks like institutional power. Ubiquitous surveillance means that it's easier for the government to round up dissidents than it is for the dissidents to anonymously organize. Data monitoring means it's easier for the Great Firewall of China to block data than it is to circumvent it. And as easy as it is to circumvent copy protection schemes, most users can't do it.

This is largely because leveraging power on the Internet requires technical expertise, and most distributed power groups don't have that expertise. Those with sufficient technical ability will be able to stay ahead of institutional power. Whether it's setting up your own email server, effectively using encryption and anonymity tools, or breaking copy protection, there will always be technologies that are one step ahead of institutional power. This is why cybercrime is still pervasive, even as institutional power increases, and why organizations like Anonymous are still a social and political force. If technology continues to advance—and there's no reason to believe it won't—there will always be a security gap in which technically savvy Robin Hoods can operate.

My main concern is for the rest of us: people who have don't have the technical ability to evade the large governments and corporations that are controlling our Internet use, avoid the criminal and hacker groups who prey on us, or join any resistance or dissident movements. People who accept the default configuration options, arbitrary terms of service, NSA-installed back doors, and the occasional complete loss of their data. In the feudal world, these are the hapless peasants. And it's even worse when the feudal lords—or any powers—fight each other. As anyone watching Game of Thrones knows, peasants get trampled when powers fight: when Facebook, Google, Apple, and Amazon fight it out in the market; when the US, EU, China, and Russia fight it out in geopolitics; or when it's the US vs. the terrorists or China vs. its dissidents.

The abuse will only get worse as technology continues to advance. In the battle between institutional power and distributed power, more technology means more damage. Cybercriminals can rob more people more quickly than criminals who have to physically visit everyone they rob. Digital pirates can make more copies of more things much more quickly than their analog forebears. And 3D printers mean that data use restriction debates will now involve guns, not movies. It's the same problem as the "weapons of mass destruction" fear: terrorists with nuclear or biological weapons can do a lot

more damage than terrorists with conventional explosives.

The more destabilizing the technologies, the greater the rhetoric of fear, and the stronger institutional power will get. This means even more repressive security measures, even if the security gap means that such measures are increasingly ineffective. And it will squeeze the peasants in the middle even more.

Without the protection of feudal lords, we're subject to abuse by criminals and other feudal lords. Also, there are often no other options but to align with someone. But both these corporations and the government—and sometimes the two in cahoots—are using their power to their own advantage, trampling on our rights in the process. And without the technical savvy to become Robin Hoods ourselves, we have no recourse but to submit to whatever institutional power wants.

So what happens? Is a police state the only effective way to control distributed power and keep our society safe? Or is government control ultimately futile, and the only hope for society an anarchic failed state run by warlords? Are there even any stable possibilities between these two poles? I don't know, but I do know that understanding the dynamics I've described in this essay is important.

We're at the beginning of some critical debates about the future of the Internet: the role of law enforcement, the character of ubiquitous surveillance, the collection of our entire life's history, the role of automatic algorithms that judge and control us, government control over the Internet, cyberwar rules of engagement, national sovereignty on the Internet, limitations on the power of corporations over our data, the ramifications of information consumerism, and so on. These are all complicated issues that require meaningful debate, international cooperation, and innovative solutions. We need to decide on the proper balance between institutional and decentralized power, and how to build tools that enable what is good in each while blocking the bad. It's not clear we're up for the task.

Today's Internet is a fortuitous accident. It came into being through a combination of an initial lack of commercial interests, government benign neglect, military requirements for survivability and resilience, and computer engineers building open systems that worked simply and easily. Battles over its future are going on right now: in legislatures around the world, in international organizations like the ITU, and in Internet organizations like the IGF. We need to engage in these debates, or tomorrow's Internet will be controlled only by those who wield traditional power.

THREE GENERATIONS OF THE NETWORKED PUBLIC SPHERE

John Kelly

Practitioners of "big data analytics" have seen their jobs get easier in some ways over the last half dozen years. Back when blogospheres were the object of study, analysts had to spend countless days writing code to scrape web pages, pull RSS feeds, parse the data, and figure out how to tell the intended prose of authors from the mechanical chatter of platforms. Just storing the results required a heavy lift of database design before one could even start collecting useable data. Now, in the era of APIs, JSON, and no-SQL databases, analysts can more easily collect a huge quantity of data and playfully explore how to work with it as the terabytes accumulate.

This (relative) ease of workflow for analysts is a side effect of great advances made in standards and code, most of it open source, that underpin the modern Web. However, the job of analysts is also harder as the object of their study—what Yochai Benkler calls the networked public sphere (NPS)—has become vastly more complicated.

Five or six years ago one could map blog activity around some issue or scope, call it a picture of the NPS, and get away with it. No longer. In the short period of time since online communications began competing with mainstream media as the primary carrier of effective discourse around public affairs, we have seen three generations in the evolution of the NPS. And the ecosystem is still evolving.

The first generation was the open Web, a.k.a. the blogosphere. Before blogs, there was a primordial soup of forums and bulletins boards, harboring active discursive life but not meaningfully connected to other online discussion spaces—hence no networked public sphere. Blogs, along with Web-native news and old media websites, created an interconnected tissue of discussion and hyperlinked reference and navigation, thus forming the foundational layer of the NPS.

The second generation came with the rise of the great global social platforms, Facebook and Twitter. While earlier platforms existed, some specific to particular parts of the world, the hegemony of these giants is the defining feature of NPS 2.0. Whereas the early blogosphere was mainly the playground of technical, media, and political elites, the second generation saw the expansion of the NPS to include vast numbers of regular folks (Facebook), connecting them in a dense global network of lightning-speed topic coordination and link trading (Twitter). The NPS now encompasses the globe and many of its people, making national publics directly visible to one another in ways they never had been before.

We are now entering the third generation of the NPS, in which some parts of the interconnected global public are looking for ways to reestablish more distinct communities. This trend is evidenced by the rise of niche platforms—the growing ranks of Tumblr, Pinterest, and the like—that allow people to collect more easily around shared interests and practices and to avoid the constant surveillance of their entire social networks. In other words, once parents and coworkers started showing up on Facebook, many people (and not just teenagers) realized they needed some less universally connected places to go.

The key thing to understand about these three generations of the NPS is that they supplement, rather than supplant, each other. Those who claim "blogs aren't important anymore because of Twitter" are way off the mark. Blogs remain critical NPS infrastructure, just as Facebook and Twitter remain hegemonic in the face of Quora and App.net. The oceans didn't empty out when life evolved onto land. The NPS is becoming more complex—its ecosystems diversifying but still interconnecting—which is why the job of understanding it is getting harder even as the job of collecting its data and applying computational analysis gets easier.

YOUTH ONLINE: DIVERSIFYING SOCIAL MEDIA PLATFORMS AND PRACTICES

Sandra Cortesi

A recent series of reports[1] by the Pew Internet & American Life Project in collaboration with the Berkman Center indicates that young users share a growing number of pictures, videos, relationship statuses, email addresses, and cell phone numbers over social media channels. In the past, much attention has been paid to information sharing practices over Facebook. However, our recent studies reveal that youth have started to diversify their use of social media platforms, although Facebook currently remains dominant.[2]

Even though 94 percent of young social media users (77 percent of all online youth) maintain a Facebook profile, a significant number of focus group participants expressed decreased enthusiasm for Facebook, citing "drama," an overabundance of mundane posts, and constraints on self-expression due to an increased adult presence. While youth are not abandoning Facebook, they are now diversifying their time spent on social media by adopting alternative platforms such as Twitter, Instagram, and Snapchat, which invite and support different forms of self-expression. In 2012, 11 percent of online youth used Instagram. Also, 24 percent used Twitter, up from 16 percent in 2011 and 8 percent in 2009. The trend toward platform diversification is also confirmed in focus groups and explained as follows by one participant:

> *Female (age 16): "And so now I am basically dividing things up. Instagram is mostly for pictures. Twitter is mostly for just saying what you are thinking. Facebook is both of them combined so you have to give a little bit of each. But yes, so Instagram, I posted more pictures on Instagram than on Facebook. Twitter is more natural."*

Photography provides a good example of platform diversification. Snapchat, a platform where each sent image only lasts for ten seconds, is often used for "silly photos," where focus group participants report making "crazy" or "awkward faces." Instagram is perceived to be a more intimate and less judgmental space than Facebook, and participants state that photos posted on Facebook are more likely to picture family and friends, whereas photos on Instagram are more likely to include food or things they saw in the world. As one participant stated,

> *Female (age 15): "If I want to post a photo I took that I think is a cool photo, I wouldn't put it on Facebook. Just because I know that other people would be like, oh look, she's posting photos. She thinks she's artsy and hipster. And I don't want to be one of those people, so I usually just go to Instagram if I want to."*

Even as youth enthusiastically adopt these new platforms and use different platforms to pursue varying purposes, they continue to be regular users of Facebook. Neither recent survey research nor focus groups gave any sign that Facebook use among young people is dropping substantially.

Taken together, recent data show how central online spaces have become in a young person's life. Services such as Facebook, Twitter, and Instagram are not only platforms over which personal information is shared. They are central nodes for creative self-expression and identity formation and

experimentation. As young users diversify their use of social media platforms, it will be interesting to learn how youth's online activities evolve and, potentially, interact with future platform design.

Additional Reading

Amanda Lenhart, Mary Madden, Sandra Cortesi, Urs Gasser, and Aaron Smith, "Where Teens Seek Privacy Advice," Pew Internet & American Life Project: Teens (2013), http://pewinternet.org/Reports/2013/Where-Teens-Seek-Privacy-Advice.aspx.

Mary Madden, "Teens Haven't Abandoned Facebook Yet," Pew Internet & American Life Project: Commentary, August 15, 2013, http://perma.cc/0fUib7aEzh5.

Mary Madden, Amanda Lenhart, Sandra Cortesi, Urs Gasser, Maeve Duggan, and Aaron Smith, "Teens, Social Media, and Privacy," Pew Internet & American Life Project: Teens (2013), http://pewinternet.org/Reports/2013/Teens-Social-Media-And-Privacy.aspx

Mary Madden, Amanda Lenhart, Maeve Duggan, Sandra Cortesi, and Urs Gasser. "Teens and Technology," Pew Internet & American Life Project: Teens (2013), http://pewinternet.org/Reports/2013/Teens-and-Tech.aspx.

Aaron Smith, "Civic Engagement in the Digital Age," Pew Internet & American Life Project: Politics (2012), http://www.pewinternet.org/Reports/2013/Civic-Engagement.aspx.

Notes

1. The reports are based on findings from a nationally representative phone survey (n=802 adults and 802 teens) and two online focus groups (n=20 teens) run by the Pew Internet & American Life Project, as well as 30 in-person focus group interviews (n=203 teens) run by the Youth and Media team at the Berkman Center.
2. Mary Madden, et al., "Teens, Social Media, and Privacy," Pew Internet & American Life Project: Teens (2013), http://pewinternet.org/Reports/2013/Teens-Social-Media-And-Privacy.aspx.