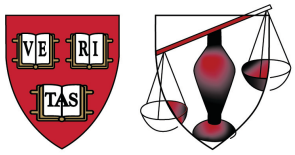


Berkman
The Berkman Center for Internet & Society
at Harvard University

Research Publication No. 2013-27
December 12, 2013

Internet Monitor 2013: *Reflections on the Digital World*

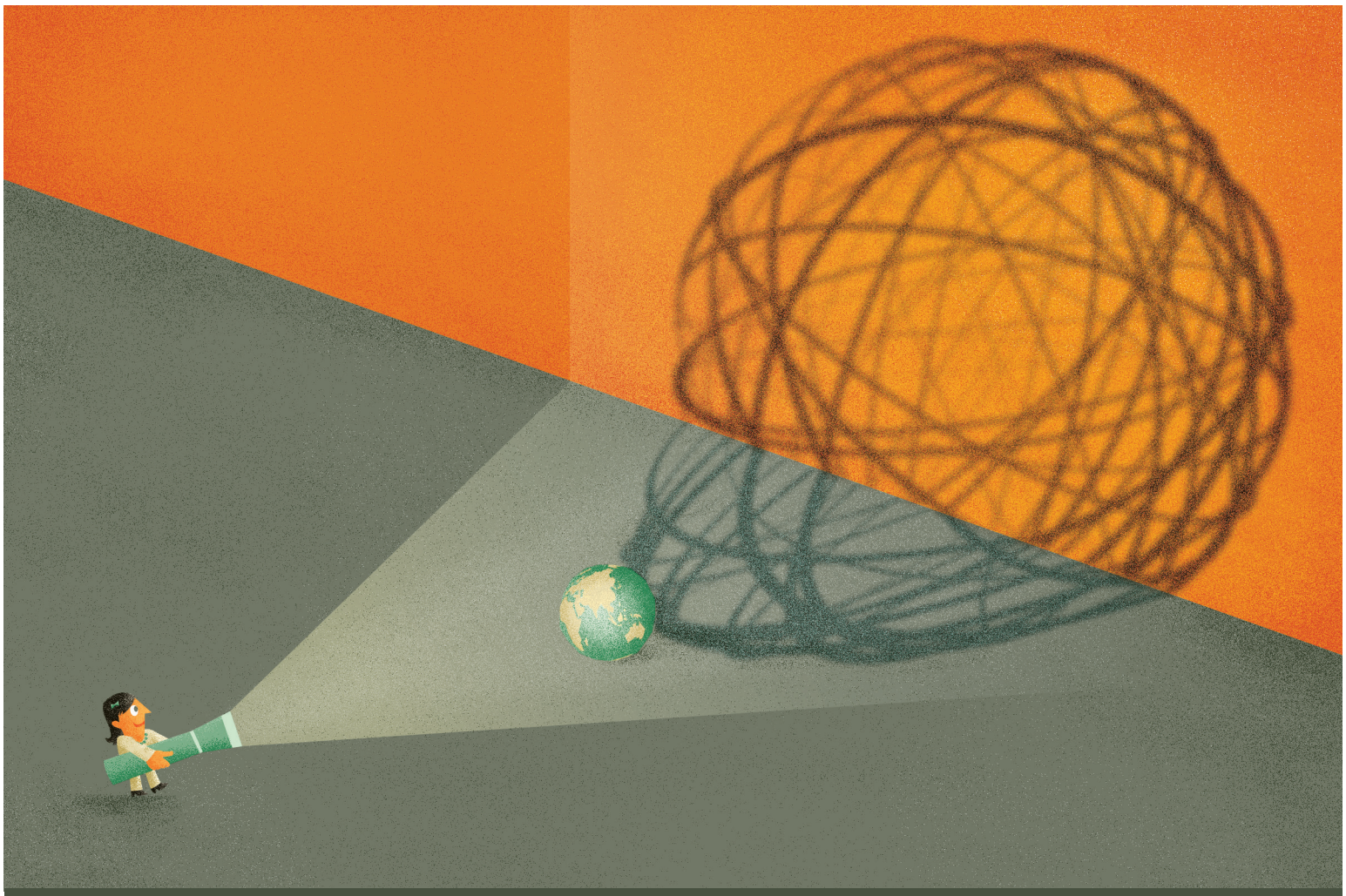
Urs Gasser
Robert Faris
Rebekah Heacock

23 Everett Street • Second Floor • Cambridge, Massachusetts 02138
+1 617.495.7547 • +1 617.495.7641 (fax) • http://cyber.law.harvard.edu •
cyber@law.harvard.edu

INTERNET MONITOR

INTERNET MONITOR 2013

Reflections on the Digital World



With contributions from: CHRISTOPHER T. BAVITZ • RYAN BUDISH • SANDRA CORTESI
MASASHI CRETE-NISHIHATA • RON DEIBERT • BRUCE ETLING • ROBERT FARIS • URS GASSER
BRYAN HAN • REBEKAH HEACOCK • JEFF HERMES • MALAVIKA JAYARAM • JOHN KELLY
PRIYA KUMAR • RONALDO LEMOS • COLIN M. MACLAY • VIKTOR MAYER-SCHÖNBERGER
HELMI NOMAN • DAVID R. O'BRIEN • MOLLY SAUTER • BRUCE SCHNEIER • WOLFGANG SCHULZ
ANDY SELLARS • ASHKAN SOLTANI • DALIA TOPELSON
REX TROUMBLEY • ZEYNEP TUFEKCI • MARK WU
and JONATHAN ZITTRAIN

Berkman
The Berkman Center for Internet & Society
at Harvard University

ACKNOWLEDGEMENTS

This report could not have come to fruition without the sustained and concerted effort of an extraordinary team. First, we wish to extend our gratitude to our authors, who graciously shared their time and expertise. We thank Bruce Etling for substantial contributions to the text and for useful and constructive recommendations on the report as a whole. We are grateful to John Palfrey for providing the impetus for the Internet Monitor project and for his thoughtful support along the way. We are indebted to Colin Maclay, who has offered untiring support, encouragement, inspiration, and sage advice throughout the development of this project.

Our special thanks to Robert Faris, who steered and shaped this report as Berkman's Research Director, as well as to Rebekah Heacock, who managed the evolution and production of this publication and provided extensive research, analytic, and editorial support. Thanks also to Adam Lewis and Elizabeth Anne Watkins for providing excellent additional research and editorial support.

We gratefully acknowledge the support of the United States Department of State and the MacArthur Foundation for the Internet Monitor project.

Urs Gasser and Jonathan Zittrain
Co-Principal Investigators

ABOUT THIS REPORT

This publication is the first annual report of the Internet Monitor project at the Berkman Center for Internet & Society at Harvard University. Instead of offering a traditional project report, and to mirror the collaborative spirit of the initiative, we compile—based on an open invitation to the members of the extended Berkman community—nearly two dozen short essays from friends, colleagues, and collaborators in the United States and abroad.

The result is intended for a general interest audience and invites reflection and discussion of the past year's notable events and trends in the digitally networked environment. Our goal is not to describe the "state of the Internet" in any definitive way, but rather to highlight and discuss some of the most fascinating developments and debates over the past year worthy of broader public conversation.

Our contributors canvass a broad range of topics and regions—from a critique of India's Unique Identity project to a review of corporate transparency reporting to a first-person report from the Gezi Park protests. A common thread explores how actors within government, industry, and civil society are wrestling with the changing power dynamics of the digital realm.

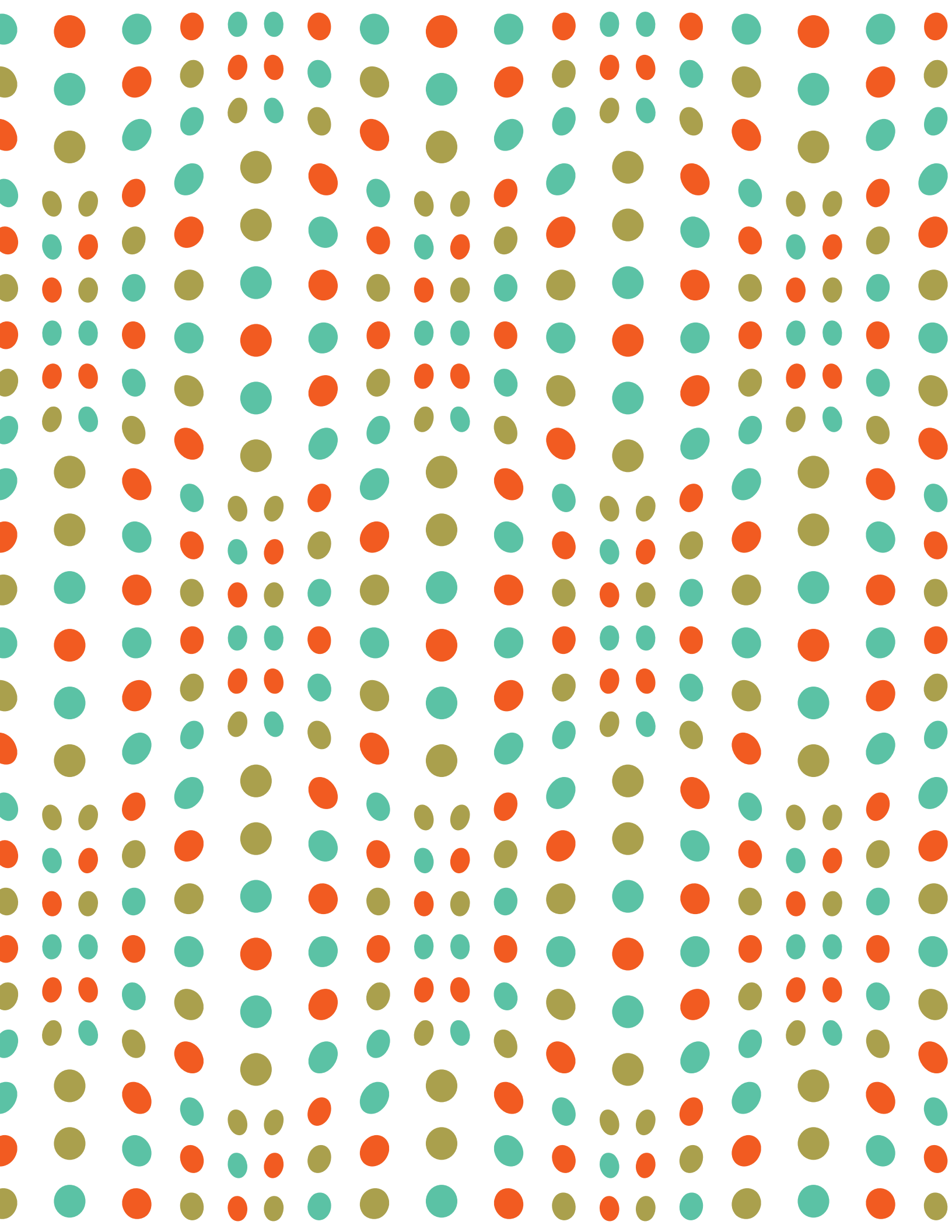
2013 has proven to be a particularly interesting year in which to produce the Internet Monitor's first annual report. For better or worse, Edward Snowden's leaks in June 2013 regarding mass surveillance programs conducted by the United States National Security Agency and its international partners have dominated nearly all subsequent discussions of the online space. While we did not set out to focus on the implications of digital surveillance, this emerged as a common theme in many of essays contributed to this publication. Whether taken individually or collectively, it is clear that the authors view the public recognition of digital surveillance as a potential game changer.

The Internet Monitor project has grown out of several key Berkman Center efforts, including the Open Net Initiative, which for over a decade has worked to investigate and analyze Internet filtering and surveillance practices around the world. These roots are evident in this report: we approach questions of privacy, security, architecture, and regulation with the goal of taking a broad view of the evolving dynamics of Internet activity and control, measuring what facilitates or hinders online expression and community formation. In describing these dynamics, we focus on the provision of physical infrastructure, the policies and actions of governments and companies, and the contributions and activities of netizens and civil society groups.

The report reflects the diversity of ideas and input the Internet Monitor project seeks to invite. Some of the essays within this report are descriptive; others prescriptive. Some of the essays are confined to factual observations and others offer personal opinion. We believe that they all offer insights and hope they will provoke further reflection, conversation, and debate in both offline and online settings around the globe.

Urs Gasser and Jonathan Zittrain
Co-Principal Investigators

TABLE OF CONTENTS



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.

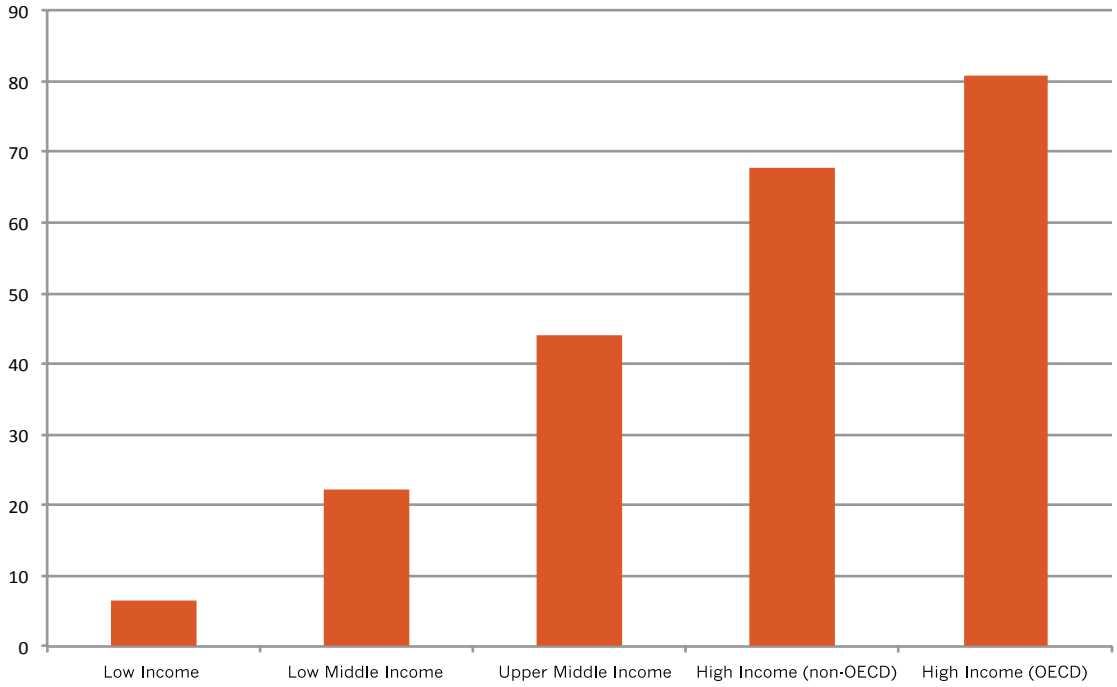


Figure 1: Percentage of individuals using the Internet (2012), by national income level

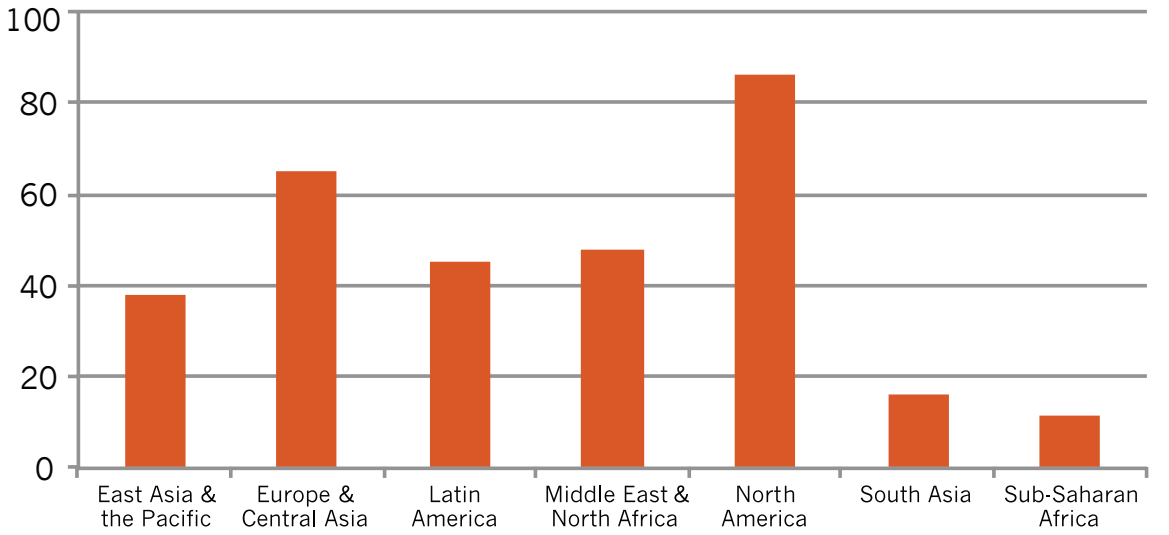


Figure 2: Percentage of individuals using the Internet (2012), by region

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.

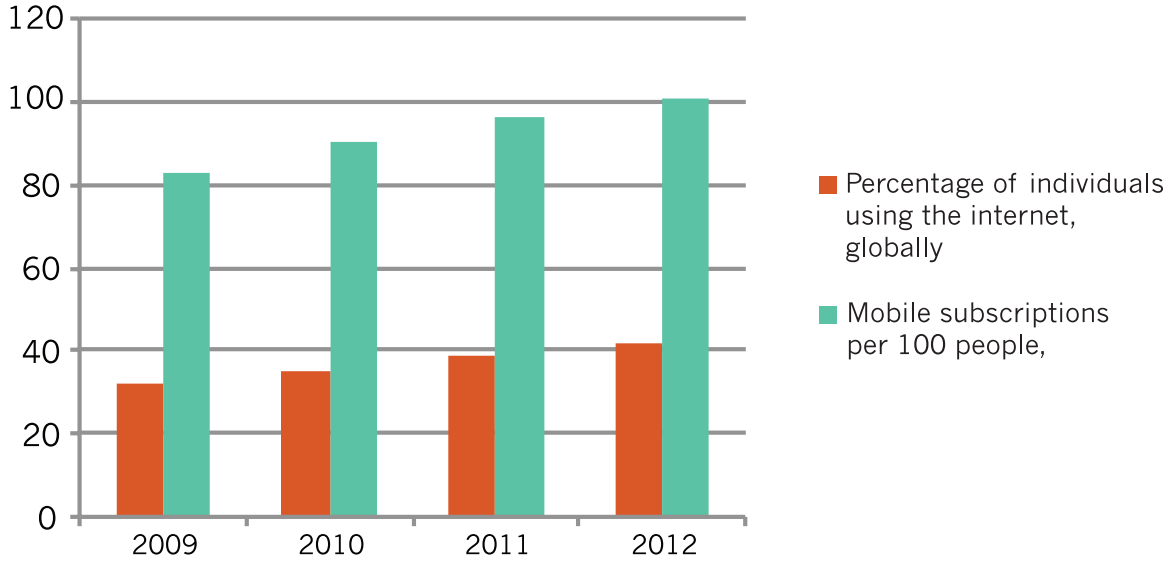


Figure 3: Mobile subscription rate vs. Internet penetration rate, global average

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.

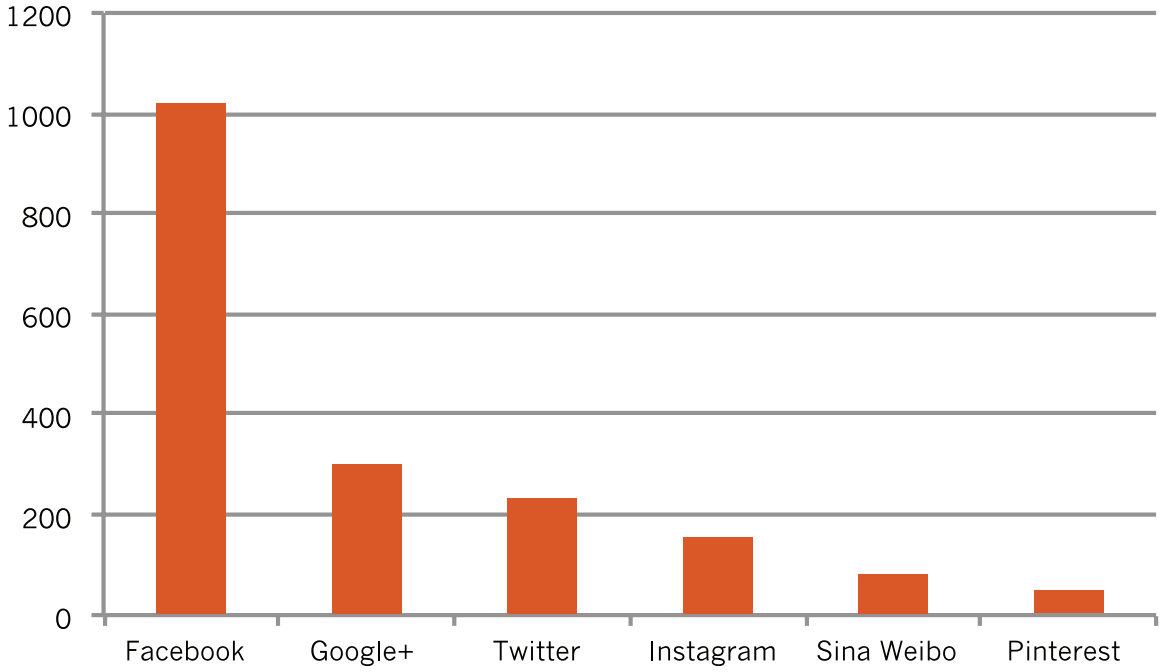


Figure 4: Monthly active users of popular social media sites (in millions)

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.

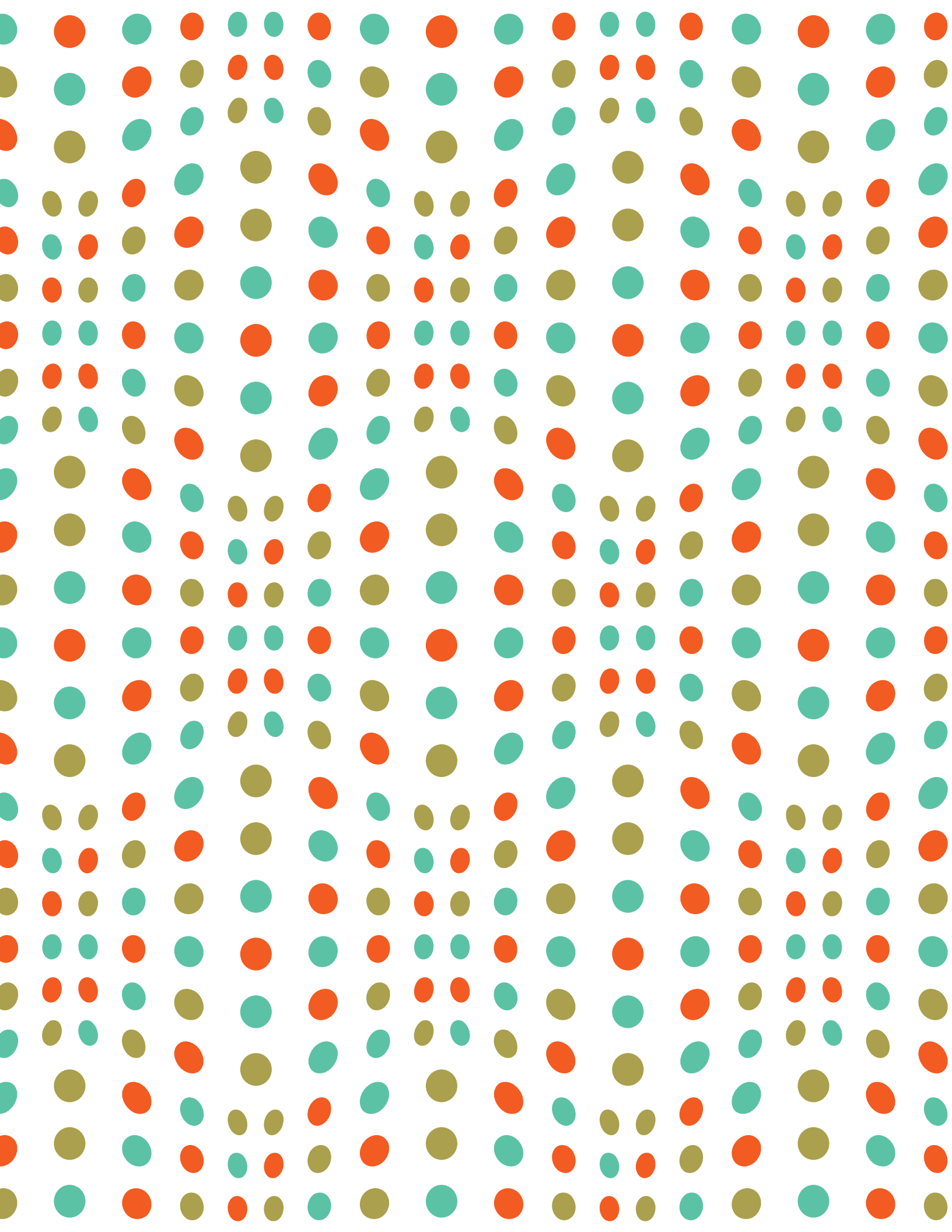
Mary Madden, Amanda Lenhart, Sandra Cortesi, Urs Gasser, Maeve Duggan, and Aaron Smith, "Teens, Social Media, and Privacy," Pew Internet & American Life Project: Teens (2013), http://pewinternet.org/Reports/2013/Teens-Social-Media-And-Privacy.aspx

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.



GOVERNMENT AS ACTORS

Robert Faris and Urs Gasser

The stakes are getting higher. As more and more citizens rely on digital technologies in their everyday lives, governments around the world face constant political pressure to address concerns over online security and harmful speech online. Concurrently, the costs of excessive regulation on innovation and civil liberties are of increasing concern. Deciding when and how to intervene in digital affairs is only getting harder for governments.

> ***Over the course of the last several years, many governments have developed policy strategies to cultivate and participate in the emerging cloud computing industry.***
>
> —DAVID R. O'BRIEN AND URS GASSER
> Cloud Computing and the Roles of Governments

The public sector has always played an important role in the evolution of the Internet. Governments have been enablers: investing in infrastructure, encouraging private sector action, conducting training and education, and setting up legal regimes to support market environments that are ripe for innovation. Governments also have acted as constrainers: reining in illegal activity, filtering speech, and inhibiting malicious behavior online. Frequently, enabling and constraining are different facets of the same policy actions; suppressing harmful activity may facilitate beneficial interactions. However, tensions and trade-offs often accompany government interventions. For example, cracking down on cybercrime may help to stimulate online business, but it may also hurt innovation. Laws and mechanisms for combating harmful speech often come at the cost of legitimate speech. Win-win scenarios are the exception.

Government action is also shaped by strategic interests. There is no shortage of governments that seek to manipulate online environments to enhance their power and limit political opposition. Separating strategic behavior from interventions taken in the public interest is difficult, as this behavior is conveniently cloaked in the rhetoric of legitimate public sector action and commonly framed in terms of law enforcement, security, and protection.

At one end of the spectrum, a few dozen countries aggressively seek to control Internet activity. This group of countries comprises primarily those that have a long history of tight media controls and authoritarian government. These governments have considerable experience in attempting to control Internet activity and have tried a wide variety of strategies, based on a few options: (1) identifying and pursuing authors and activist networks that reside domestically, taking down content hosted domestically; (2) blocking content hosted overseas (this is often coupled with pressure on foreign countries and cyber-attacks); (3) engaging in information campaigns to disrupt online discussions and promote government-friendly messaging; and (4) limiting access to the Internet altogether.

Despite many years of concerted efforts, the difficulty of enforcing information controls on the Internet continues to vex governments that are intent on limiting online communication. The scale of the Internet, along with its distributed architecture and the ability to at least partially cloak one's identity

online, make locating the source of objectionable speech and blocking the spread of unwanted content a formidable task. In an attempt to increase enforcement capacity, countries draw on a number of common strategies, including: (1) enlisting the help of intermediaries in blocking content and accessing identifying information; (2) conducting surveillance; (3) compelling domestic hosting; (4) enacting licensing and real name requirements; and (5) passing legislation that is sufficiently broad to provide a rationale and to facilitate implementation of the above.

Ultimately, the effectiveness of these policies is manifest in self-censorship—increasing the costs and risks of engaging in digital communication discourages more and more individuals from writing about controversial topics online. Self-censorship is particularly difficult to measure; we are unable to observe that which does not occur, though we might make inferences about types of content that are unrepresented or missing online.

After witnessing a rapid increase in the number of countries that developed national-level content filtering during the first decade of the 21st century (there are currently several dozen, depending on how one counts), we have seen fewer big shifts in recent years. By and large, those that are able to garner the political power to implement Internet filtering are now doing so. Burma and Tunisia have notably scaled back their filtering regimes over the past two years. Russia has begun to block sites related to extremist thought and to pornography, drugs, and satire, and earlier this year, Jordan instigated blocking of hundreds of websites that did not comply with new online media licensing requirements. Pakistan is caught up in an ongoing policy dispute over plans to scale up filtering. The UK recently joined the ranks of countries that turned back serious attempts to enact broad scale filtering, following a similar path to Australia several years earlier. In Iran, statements that signal a possible softening of Internet filtering, along with the fact that officials in the current administration—including the president—maintain active Facebook and Twitter accounts (both platforms are blocked in the country), highlights the diverging opinions within the government on the current filtering policy and the possibility of controls being loosened in the future. Perhaps the most interesting and potentially pernicious control strategies are China's efforts to control speech in social media.

> ***Over the past several years, microblogging has emerged as the heart and soul of a remarkably vibrant networked public sphere in China. For government censors, this represents a challenging task.***
>
> —ROBERT FARIS
> Policing Social Media in China

The challenge of enforcing content restrictions on sites hosted outside of the country is not easily surmounted. Several countries have tried with little success to force social media and content hosting platforms to maintain a domestic presence that is within the reach of local control. China continues to be a notable exception after using a combination of laws and the blocking of outside platforms to create a social media market dominated by domestic firms. Attempts to convince foreign-based platforms to adopt local content restriction policies have yielded limited success. YouTube has agreed to geographic blocking of some videos; Google has agreed to remove results from country-specific versions of its search engine, and Twitter has set up a process for blocking tweets that are illegal

according to national laws. In general, these steps fall far short of the aspirations of many regulators. A handful of countries, including Thailand, Pakistan, Turkey, and Vietnam, have resorted to blocking entire platforms for long periods of time without prompting the emergence of local alternatives.

The apparent slowing of the spread of filtering does not necessarily translate into generally good news for the state of civil liberties online. Pursuing individuals through legal and extralegal means continues be a mainstay of control strategies that all too frequently impinge on basic human rights. The number of authors behind bars for their online writing continues to grow. Over the past several months, China and Vietnam, in particular, have arrested a large number of bloggers and microbloggers.

Cyberattacks have been employed in apparent efforts to influence content hosted abroad, though their use is problematic. Given the shaky ethics and merits of this approach, governments that do support and carry out such actions are not eager to take credit and must limit their level of involvement to maintain a measure of deniability. It is unclear that the associated service disruptions have a substantial long-term impact. Hacking into servers is potentially more serious when it uncovers sensitive personal information; this is where hacking ties with surveillance.

> ***Edward Snowden's disclosure of National Security Administration surveillance practices has provoked a public debate about the merits of establishing an international standard for privacy and data protection.***
>
> —WOLFGANG SCHULZ
> After Snowden: Toward a Global Data Privacy Standard?

In the past year, we have learned much about the mechanisms and scope of digital surveillance, particularly as carried out by the NSA. It is logical to assume that the US government has a sizable advantage over other countries in its technical expertise and access to information flows. It is also reasonable to assume that the implied principles of digital surveillance—as suggested by NSA practices—are the same around the world: capture as much information as possible, by any available means. This is due in part to structural changes that may not be reversible. In prior generations, the cost of surveillance and data acquisition constituted a useful buffer between state surveillance and privacy; resource constraints forced law enforcement to focus on a limited number of targets on a scale where judicial oversight was a practical—if imperfect—deterrent against overreach.

Both cyberattacks and surveillance represent threats to a related set of principles of democratic governance: accountability and transparency. The prospect of governments working in the shadows greatly hinders efforts to document and analyze these activities and to design governance and accountability systems that include adequate oversight.

Over the past couple of years, lawmakers have endeavored to define the contours of permissible speech online and support the development of legal and administrative mechanisms for implementing regulations. Among the troubling examples of this legislative activity are the rumor regulations enacted in China that criminalize the spread of information deemed defamatory or in some way inaccurate (the regulations do not define what constitutes a rumor, leaving interpretation open to authorities). In

Vietnam, Decree 72 restricts blogs and social websites to content related to 'personal information,' leaving discussion of news and current events in the realm of forbidden speech. Recent changes to media law in Jordan require websites that include news and commentary related to Jordan to be licensed by the government. Amendments to Bangladesh's ICT law made in August 2013 criminalize "publishing fake, obscene[,] or defaming information," or posting materials that "prejudice the image of the State" or "hurt religious belief."

Noting that intrusive filtering comes at a political cost, even for authoritarian regimes. Rather than maintaining constant filtering regimes, an increasing number of countries are cranking up controls for shorter periods of time during times of unrest or political sensitivity such as protests or elections. China and Iran have historically dialed up content controls for periods of time. At an extreme, blacking out the Internet has become a more common short-term tool and has been implemented in Egypt, Libya, Syria, and Sudan.

> ***"On June 14, 2013, Iran held presidential elections, the first since massive protests rocked the country after former President Mahmoud Ahmadinejad's reelection in 2009. As with previous elections, this event was preceded by a period of extensive Internet censorship and general bandwidth restrictions, a phenomenon known as "just-in-time blocking."***
>
> —RYAN BUDISH AND PRIYA KUMAR
> Just in Time Censorship: Targeted Internet Filtering During Iran's 2013 Elections"

In countries committed to protecting online speech, the nature of regulatory challenges is different. Drawing a clean line between protected and unprotected speech is impossible, and processes for adjudicating the difficult cases get bogged down when operating at the scale of the Internet. A core problem is that increasing the effectiveness of measures to squash unprotected speech online endangers protected speech and threatens the development of a vibrant space for collaboration and innovation. A related concern is that the legal, administrative, and technical structures used for legitimate regulatory action are easily extended to levels that trample civil liberties and blunt the benefits of economic, political, and social activity online. In many countries, comprised largely of strong democracies, an appreciation for these tensions has supported policies characterized by regulatory restraint and prompted the passage of laws and policies that affirmatively build in speech protections. This represents a stark contrast to countries that aggressively constrain online communication.

The treatment of intermediary liability is perhaps the best single indicator of the tone and general disposition to online speech—the countries that require intermediaries to police content on their platforms also tend to employ other strategies to restrict online content and activity, and those that limit intermediary liability have the most active online environments.

However, promoting productive online activity is by no means straightforward, and for governments that seek to promote greater online engagement among their citizens, a number of difficult policy challenges lie ahead. Among these is resolving a host of complex issues related to cloud computing, which will be difficult both in the West and in less open environments.

Net neutrality and broadband policy debates are tangled up in the age old ideological disputes over the proper role of government and standards for intervening in private markets. These philosophical differences extend as well to debates over privacy. Many privacy advocates expect governments to play a more proactive role in crafting online privacy protections, though others favor a hands-off approach. The EU is taking a leading role in defining mechanisms to protect privacy. The complexities of transnational data flows again come into play in the realm of privacy, as conflicting privacy regimes may impede access to outside platforms and data services. Harmonization of these regimes into a global data privacy standard is one possible solution that has gotten a boost from the NSA surveillance controversy.

> ***China may be home to the most Internet users in the world and increasingly sophisticated Internet companies, but when it comes to unleashing the potential of cloud computing, China lags behind.***
>
> —MARK WU
> China Moves to the Cloud

> ***Arguably the most important legislative activity in the privacy field this past year unfolded in the European Union.***
>
> —VIKTOR MAYER-SCHÖNBERGER
> Data Privacy Reform in the European Union

The regulatory approaches of the BRIC countries—Brazil, Russia, India, and China—reflect much of the variation in Internet strategies. China continues to set the standard for applying an extensive and multi-pronged approach to keeping a lid on digital activism that employs legal, technical, and social control mechanisms. Yet online discussions and debates in China are extremely active and take on a very wide range of issues and debates not featured in traditional media. Russia has traditionally relied upon non-filtering methods, including offline intimidation of journalists and the threats of legal action and surveillance, while allowing political discussion online to flourish. In both China and Russia, we see evidence that governments are more concerned with political organizing online that they are with freedom of speech and criticism of the government, although the two are inextricably linked. While government filters can slow the diffusion of information, attempts to prevent the distribution of ideas, memes, articles, and videos online have proven to be futile. Civil society organizing online, however, is both a bigger threat to non-democratic and semi-democratic regimes and easier to disrupt. In both China and Russia, the approach appears to be focused on dismantling emergent efforts at social mobilization before they take hold. This is often achieved by targeting key hubs and leaders, while allowing a good degree of political debate to continue.

> ***In 2008, India's Information Technology Act was amended to allow for broad government control and authority over the Internet in many circumstances.***
>
> —CHRISTOPHER T. BAVITZ AND BRYAN HAN
> India's Information Technology Act

> ***If fully implemented, India's Unique Identity system will fundamentally alter the way in which citizens interact with the government by creating a centrally controlled, technology-based standard that mediates access to social services and benefits, financial systems, telecommunications, and governance.***
>
> —MALAVIKA JAYARAM
> India's Identity Crisis

India and Brazil have much stronger commitments to freedom of speech, while diverging in interesting ways from the policies adopted in North America and Europe. India has adopted the safe harbor provisions for intermediaries that played a key part in the emergence of the Internet. The same body of law also opens up a broad range of speech to possible criminal liability and gives the government broad authority to order the blocking of Internet content. India has also taken large steps to implement a national-level government identification scheme meant in part to facilitate the provision of government services and engagement in economic activity, including to many of those most in need. This initiative collides with a host of difficult privacy issues that remain unresolved. Brazil has at times adopted policies that many would describe as heavy-handed. Yet Brazil has also experimented with some of the world's most innovative and progressive approaches for engaging citizens in government decisions using digital tools. If passed into law, the Marco Civil da Internet in Brazil would perhaps represent the world's most extensive legal assertion of individual online rights.

> ***If approved in its original draft, Marco Civil will be an example of a positive, rights-enabling legislation, capable of influencing other countries.***
>
> — RONALDO LEMOS
> Marco Civil

The diversity of regulatory approaches to the Internet around the world is now sufficiently broad and long that lessons can be reasonably inferred with reasonable confidence. The policies adopted by many governments designed to protect online speech, enable the emergence of collective action, and promote business activity have had a strong positive influence on private sector and civil sector activity. Laws and policies meant to provide online security and limit harmful speech have been less successful and have often come at the cost of stunting the development of social capital online, although in many cases this was the very objective

CLOUD COMPUTING AND THE ROLES OF GOVERNMENTS

David R. O'Brien and Urs Gasser

Governments around the world increasingly engage with cloud computing—an umbrella term for an emerging trend in which many aspects of computing, such as information processing, collection, storage, and analysis, have transitioned from localized systems (i.e., personal computers and workstations) to shared, remote systems (i.e., servers and infrastructure accessed through the Internet.)[1] Cloud computing delivers several overlapping benefits that together distinguish it from traditional modes of IT consumption: computational resources are elastic and can be provisioned to many simultaneous remote users and scaled up or down with demand; services can be sold in economically efficient, pay-as-you-go models, much like a utility service; and operational expertise, including IT management and maintenance, can be outsourced to the cloud-service providers.[2]

Industry proponents herald these developments as the next big thing, and it appears that governments are listening. Over the course of the last several years, many governments have developed policy strategies to cultivate and participate in the emerging cloud computing industry. After reviewing a number of these strategies—led by governments in the US, UK, EU, and Japan—we observed that governments assume, implicitly or explicitly in executing their cloud initiatives, six distinct yet overlapping roles towards cloud computing: users, regulators, coordinators, promoters, researchers, and service providers.[3]

As users, governments take advantage of the technical flexibility and collaborative features of cloud computing by replacing their legacy IT software and hardware with cloud services managed by government employees and private-sector contractors such as Google, Amazon, and Microsoft.[4] As regulators, governments use legislative, judicial, and executive mechanisms to constrain and empower individuals, companies, and others working in the cloud computing industry. As coordinators, they actively participate in the development of technical standards, facilitate information sharing between the public and private sectors, and encourage industry players to build consortiums to coordinate interests.[5] As promoters, governments publicly endorse cloud computing technologies not only by adopting them as users and encouraging the public to adopt them, but also by incubating and funding new and existing companies.[6] As researchers, they conduct and fund public and private research initiatives that aim to understand the technical and societal challenges that the new technology presents.[7] Lastly, as providers, governments are offering cloud-related services both to the public and to other branches of government.[8]

Although it is too soon to draw conclusions about the effectiveness or appropriateness of the different roles that governments may play, a number of early observations concerning the scope of these roles are worth noting.

Based on the rationales stated in their cloud strategies, governments' objectives related to cloud computing are multifaceted—for instance, they seek to reduce their IT spending, encourage the development and use of innovative products, and foster their industries' international competitiveness. The scope of these objectives, which can vary between countries and even levels within a government, are also shaped by contextual factors, such as politics, the economy, and cultural backdrops. Governments have a wide range of policy tools at their disposal, which they can tailor to the particular roles they choose to assume and the objectives they seek to achieve.[9] For example, as coordinators and

researchers, governments can use public-private partnerships to identify areas where policy measures can be improved and to facilitate the development of technical standards in private industry.[10] As promoters of the industry, governments can strategically use government financial stimulus programs to encourage the development of new companies and to help existing companies and markets become more competitive on a global level. These policy tools and roles are not necessarily new observations, but the high degree of strategic coordination between the tools and the roles, whether deliberately planned or an emergent behavior, is noteworthy. In historical examples, government interventions in emerging technologies are often more subtle and involved fewer of the roles described in this context.

Governments are encountering challenges as they implement their strategies, particularly as they attempt to balance competing objectives across the six roles.[11] As governments become users of cloud computing services, for example, they implicitly promote individual companies and the industry as a whole by providing a lucrative revenue stream and by publicly demonstrating approval of the technology. On the other hand, a government's promotion of cloud computing can frustrate its objectives in other roles and raise questions about impartiality. Consider a case in which one branch of government promotes cloud computing for use by consumers and companies at the same time that the regulatory branch of government publicly scrutinizes the privacy and security practices of cloud computing companies.[12] Such a situation results in rather confusing public messages that may undermine government action in either role. The complexities of information sharing among different government actors or hasty policymaking may be partly to blame for such collisions.

Government strategies around cloud computing also convey a striking sense of urgency, and this perhaps provides some clues about how governments perceive the importance of the cloud computing trend. If the predictions from analysts and industry proponents are accurate, then cloud computing is poised to profoundly change how technology products and services are produced and consumed.[13] Computational resources will be more readily available to individuals and companies in developing regions of the globe, which may catalyze growth in commerce internationally. The countries with the most successful cloud industries may accumulate not just economic prosperity but also increased power, particularly since the centralized nature of cloud computing systems can serve as means to exert control over the flow of information.[14] Other factors, such as recent controversies involving international government surveillance, also appear to be punctuating the desire for stronger domestic cloud industries and legislative protections in countries around the world.[15]

Governments have a long history of intervening in emerging industries, often with mixed results. At this early stage, the impact of government cloud computing initiatives is far from clear.[16] But as they become more deeply involved, governments may find it increasingly difficult to balance their involvement in these roles while maintaining the trust of the public.[17]

Notes

1. Michael Armbrust et al., "Above the Clouds: A Berkeley View of Cloud Computing," UC Berkeley Reliable Adaptive Distributed Systems Laboratory, Technical Report No. UCB/EECS-2009-28, February 10, 2009, http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf; Peter Mell and Timothy Grance, "The NIST Definition of Cloud Computing," US National Institute for Standards and Technology (NIST), Special Publication 800-145, September 2011, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.
2. Ibid.
3. For an in depth overview of these roles and their implications, see Urs Gasser and David

O'Brien, "Governments and Cloud Computing: Roles, Approaches, and Policy Considerations," forthcoming 2013.

4. See, e.g., Vivek Kundra, Federal Cloud Computing Strategy, US Office of Management and Budget, (Washington, DC: February 8, 2011), http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/federal-cloud-computing-strategy.pdf; UK Government, Cabinet Office, Government Cloud Strategy, (London: March 2011), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/85982/government-cloud-strategy_0.pdf; European Commission, Unleashing the Potential of the Cloud in Europe, (Brussels: September 27, 2012), http://ec.europa.eu/information_society/activities/cloudcomputing/docs/com/com_cloud.pdf.

5. See, e.g., NIST, "Cloud Computing Program," http://www.nist.gov/itl/cloud/; "'Cloud Testbed Consortium' Established," Japanese Ministry of Internal Affairs and Communications press release, December 16, 2011, http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Releases/Telecommunications/11121604.html; "Digital Agenda: Tech CEOs and leaders kickstart new EU cloud computing board," European Commission press release, November 19, 2012, http://europa.eu/rapid/press-release_IP-12-1225_en.htm.

6. Florence de Borja, "Cloud Computing Companies Get Funding in France," Cloud Times, September 19, 2012, http://cloudtimes.org/2012/09/19/cloud-funding-france/.

7. See, e.g., "The Sky Is No Limit: 13 Research Teams Compete in the Clouds," National Science Foundation press release, April 20, 2011, http://www.nsf.gov/news/news_summ.jsp?org=NSF&cntn_id=119248&preview=false; European Commission, "Cloud Computing Related Research," January 2012, http://ec.europa.eu/information_society/activities/cloudcomputing/docs/cloudcomputing_related_research_20120112_full.pdf; Vivek Kundra, "Tight Budget? Look to the 'Cloud'," New York Times, August 31, 2011, http://www.nytimes.com/2011/08/31/opinion/tight-budget-look-to-the-cloud.html.

8. See, e.g., Andy Greenberg, "IBM's Chinese Cloud City," Forbes, July 28, 2009, http://www.forbes.com/2009/07/27/ibm-china-computing-intelligent-technology-ibm.html.

9. Gasser and O'Brien, "Governments and Cloud Computing."

10. See, e.g., NIST, "Cloud Computing Program," http://www.nist.gov/itl/cloud/; NIST, "Useful Documents for Cloud Adopters," http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/Documents.

11. For more detailed analysis, see Gasser and O'Brien, "Governments and Cloud Computing."

12. See, e.g., Paul Taylor, "Cloud computing industry could lose up to $35bn on NSA Disclosures," Financial Times, August 5, 2013, http://www.ft.com/cms/s/0/9f02b396-fdf0-11e2-a5b1-00144feabdc0.html; Stephanie Condon, "FTC Questions cloud-computing Security," CNET, March 17, 2009, http://news.cnet.com/8301-13578_3-10198577-38.html.

13. See, e.g., "Gartner Says Worldwide Public Cloud Services Market to Total $131 Billion," Gartner press release, February 28, 2013, http://www.gartner.com/newsroom/id/2352816; see also Louis Columbus, "Gartner Predicts Infrastructure Services Will Accelerate Cloud Computing Growth," Forbes, February 19, 2013, http://www.forbes.com/sites/louiscolumbus/2013/02/19/gartner-predicts-infrastructure-services-will-accelerate-cloud-computing-growth/.

14. See Bruce Schneier, "The Battle for Power on the Internet," The Atlantic, October 24, 2013, http://www.theatlantic.com/technology/archive/2013/10/the-battle-for-power-on-the-internet/280824/.

15. Glenn Greenwald and Ewen MacAskill, "NSA Prism program taps in to user data of Apple, Google, and others," The Guardian, June 6, 2013, http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data; Jordan Novet, "PRISM could foil the public-cloud campaign, and private clouds might lie in crosshairs," GigaOm, June 17, 2013, gigaom.com/2013/06/17/prism-could-foil-the-public-cloud-campaign-and-private-clouds-might-lie-in-crosshairs/.

16. See, e.g., Fred Block and Matthew Keller, eds., State of Innovation: The US Government's Role in Technology Development (London: Paradigm Publishers, 2011).

17. See, e.g., Rachel King, "NSA's Involvement in Standards Setting Erodes Trust," Wall Street Journal, October 1, 2013, http://blogs.wsj.com/cio/2013/10/01/nsas-involvement-in-standards-setting-erodes-trust/; NIST, "Cryptographic Standards Statement," September 10, 2013, http://www.nist.gov/director/cybersecuritystatement-091013.cfm.

POLICING SOCIAL MEDIA IN CHINA

Robert Faris

China is renowned for its lukewarm embrace of the open Internet and its willingness to go to great lengths to curtail online speech. Its longstanding Internet filtering apparatus, the so-called Great Firewall, is intended to prevent users from accessing thousands of websites hosted outside of China. This centrally coordinated system is based on maintaining a running list of keywords and web addresses to be blocked. In technical terms, it is quite sophisticated. In terms of content control, it is crude; thousands of innocuous sites are caught up by the keyword-based logic, while much controversial content continues to leak through. Amid the thousands of keywords and web addresses on the block list, the blocking of a handful of social media sites—Facebook, Twitter, YouTube, and various blog hosting platforms—has arguably had the biggest impact on the Internet in China by ensuring that domestic firms have come to dominate social media markets in China. This means that control of social media content in China is a domestic affair.

Over the past several years, microblogging has emerged as the heart and soul of a remarkably vibrant networked public sphere in China. Social media in China is staggering in scale, both in the number of participants (registered accounts are currently estimated at about half a billion) and in the breadth of topics that are discussed. For government censors, this represents a very different and far more challenging task.

A number of studies over the past year have shed a great deal of light on the mechanisms that are employed in China. The first step is holding the intermediaries responsible for the content that passes through their platforms. This in turn has prompted software companies to produce tools for social media sites to support a hybrid approach in which technical filters flag content for subsequent human review. This approach offers a more fine-grained approach to blocking content that incorporates human judgment, but at a cost. Back of the envelope calculations suggest that social media companies employ tens of thousands of people to manually review individual posts.[1]

Among the estimated one hundred million posts each day, a substantial number never make it through the review process for public viewing. And for those that survive the initial technical screen, studies estimate that another 10-15 percent of posts are subsequently taken down. These activities leave a digital record that allows researchers to study the targeting of social media censorship. The evidence supports the view of a system that allows discussion of many controversial topics, but responds quickly and decisively to prevent selected topics from catching fire in digital media. The surprising twist is that criticism of the government is apparently not a factor in social media censorship. Many posts that are highly critical of the government are allowed online as long as they are not related to hot button topics, while posts that are supportive of government positions are taken down if related to the most sensitive issues.

This is partial vindication for those who believed that preventing ideas from being spread via the Internet would prove to be impossible: technology is triumphing over the political will of repressive governments. However, it supports the notion that authoritarian regimes fear collective action above all else. The most recent wave of blogger arrests, which includes many high profile bloggers, is a sign

that the government is wary of the power of social media in China, despite the massive monitoring and take-down regime in place. It also points to the inherent fragility of civil society action online.

Additional Reading

Gary King, Jennifer Pan, and Margaret Roberts, "How Censorship in China Allows Government Criticism but Silences Collective Expression," American Political Science Review 107, no. 2 (2013): 1-18, http://gking.harvard.edu/publications/how-censorship-china-allows-government-criticism-silences-collective-expression.

Tao Zhu, et al., "The Velocity of Censorship: High-Fidelity Detection of Microblog Post Deletions," July 10, 2013, http://arxiv.org/abs/1303.0597.

David Bamman, Brendan O'Connor, and Noah Smith, "Censorship and deletion practices in Chinese social media," First Monday 17, no. 3 (2012), doi:10.5210/fm.v17i3.3943.

Notes

1. Gary, Jennifer Pan, and Margaret Roberts, " A Randomized Experimental Study of Censorship in China," October 6, 2013, http://gking.harvard.edu/publications/randomized-experimental-study-censorship-china.

AFTER SNOWDEN: TOWARD A GLOBAL DATA PRIVACY STANDARD?

Wolfgang Schulz

Edward Snowden's disclosure of National Security Administration surveillance practices has provoked a public debate about the merits of establishing an international standard for privacy and data protection. Officials from a number of countries, including Brazil, Uruguay, Denmark, Holland, and Hungary, have expressed interest in such a standard. Perhaps the most intriguing development thus far is a proposal by Germany's federal data protection officer, Peter Schaar, who has proposed adding a protocol to Article 17 of the United Nations' International Covenant on Civil and Political Rights, which protects against "arbitrary or unlawful interference with…privacy, family, home or correspondence."[1] This proposal, and the debate that accompanies it, have raised two key questions: 1) Is creating an enforceable global privacy standard even possible?; and, 2) If so, what form should this standard take?

Discussions about a global privacy standard predate the Snowden leaks. That being said, the current debate is very much grounded in the context of the Snowden controversy. Revelations of comparable prominence and scope (such as the Wikileaks releases of 2010) have historically had adverse effects on efforts to further secure the privacy of Internet users. Governments made to feel vulnerable by revelations of this nature sometimes respond defensively by cracking down on leakers and finding other ways to increase government access to information while reducing transparency. Furthermore, media coverage of past controversies has framed these leaks in the context of "leakers versus the government," pushing advocates on both sides of the issue (as well as members of the public) toward extreme positions that hinder productive discussion and policy development.

Despite this challenging context, a number of resources exist that may help inform the current discussion. In the last few years, a specialized subset of academic discourse has centered on global data privacy standards.[2] One notable scholar in this field, Australian law professor Graham Greenleaf, has outlined an approach that differs from Schaar's protocol addendum in one key aspect: instead of involving the UN, he proposes building on the Council of Europe's (CoE) existing Data Protection Convention 108. The arguments against and in support of Greenleaf's proposal may be indicative of arguments that will surround Schaar's proposed amendment to the ICCPR.

Although it is an established practice for non-CoE countries to sign such conventions, critics of Greenleaf's approach argue that there are few apparent incentives for the US government to do so at this time. Furthermore, from a privacy advocate's standpoint, creating a global data privacy standard comes with the risk of starting a "race to the bottom." This theory holds that as soon as a widespread data privacy treaty is in force, states with greater protective measures would have to justify why their measures exceed global standards. Studies suggest, however, that this fear is unfounded. Greenleaf himself has demonstrated that data privacy laws have a global trajectory that increasingly favors expanding protections rather than rolling them back. He adds that the primary principles shaping this trajectory draw on the EU Directive more than any other source.[3]

Greenleaf's arguments, and those of other optimistic advocates of increased data protection, are further bolstered by trends in the private sector driven by greater public demand for data protection.

A primary example of this is how some IT companies, rather than viewing data protection standards as a state-imposed cost, are emphasizing privacy protection as a key selling point to consumers. In Germany, for instance, Internet service providers now advertise the fact that they encrypt email communication. These trends indicate that a shift to high data protection standards could be supported not only by government forces but also by private sector companies that wish to cater to public demand.

Given these developments, there is good reason to believe that a global standard for data privacy could be created and enforced. Determining what this standard should look like, who should be responsible for enforcing it, and what power it will actually have to shape the continuing evolution of the Internet will require further scholarship and debate. Academia can play a pivotal role in this process by generating research to focus the problem, creating and evaluating public and private solutions, and providing a platform for debate.

As the conversation moves from scholarship to policy creation, the ITU could serve as a suitable platform for negotiations, especially when paired with UNESCO involvement to monitor implications for freedom of speech. But it may also be necessary to think creatively about negotiating a new treaty independent of established UN institutions—a similar process was used to create the Rome Statute, which serves as the basis for the International Criminal Court.

The process of creating a global standard for data privacy requires an undeniably delicate balancing act that must negotiate a complex interplay of technological, social, economic, legal, and political factors. It is a process, however, that offers the chance to create a healthier Internet where all global citizens can enjoy the benefits of interconnectivity without unduly compromising their own security. While success may be uncertain, this goal is definitely worth pursuing.

Notes

1. Peter Schaar, "Prism und Tempora: Zügellose Überwachung zurückfahren!," *Der Spiegel*, June 25, 2013, http://www.spiegel.de/netzwelt/netzpolitik/peter-schaar-zu-prism-und-tempora-ueberwachung-zurueckfahren-a-907793.html. See also: International Covenant on Civil and Political Rights (ICCPR), adopted December 16, 1966, G.A. Res. 2200A (XXI), 21 U.N. GAOR Supp. (No. 16) at 52, U.N. Doc. A/6316 (1966), 999 U.N.T.S. 171, entered into force March 23, 1976, http://treaties.un.org/doc/Publication/UNTS/Volume%20999/volume-999-I-14668-English.pdf, art. 17.
2. Graham Greenleaf, "Uruguay Starts Convention 108's Global Journey with Accession: Toward a Global Privacy Treaty?" *Privacy Laws & Business International Report,* Issue 122, 20-23 (April 2013), Research Paper No. 2013-38, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2280121; Haksoo Ko, "Law and Technology of Data Privacy: A Case for International Harmonization," *Seoul National University School of Law*, June 13, 2012, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2083602; Alessandro Mantelero, "Data Protection in a Global World," *Polytechnic University of Turin - Nexa Center for Internet & Society*, June 20, 2012, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2087987.
3. Graham Greenleaf, "Global Data Privacy in a Networked World," in *Research Handbook on Governance of the Internet*, ed. I. Brown and Edward Elgar, 2012, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1954296.

JUST IN TIME CENSORSHIP: TARGETED INTERNET FILTERING DURING IRAN'S 2013 ELECTIONS

Ryan Budish
Priya Kumar contributed to this report

On June 14, 2013, Iran held presidential elections, the first since massive protests rocked the country after former President Mahmoud Ahmadinejad's reelection in 2009. As with previous elections, this event was immediately preceded by a period of extensive Internet censorship and general bandwidth restrictions, a phenomenon known as "just-in-time blocking."[1] In the month surrounding the elections, Herdict, a platform that collects crowdsourced data about inaccessible and censored websites, and ASL 19, an anti-censorship advocacy organization, partnered to monitor the extent of the censorship.

During the partnership, ASL 19 asked Iranian users of the Psiphon circumvention tool to report inaccessible websites to Herdict. Between June 1 and July 1, 2013, Herdict received 3,533 reports from Iran that provide a unique look at Iranian censorship immediately before and after the election.

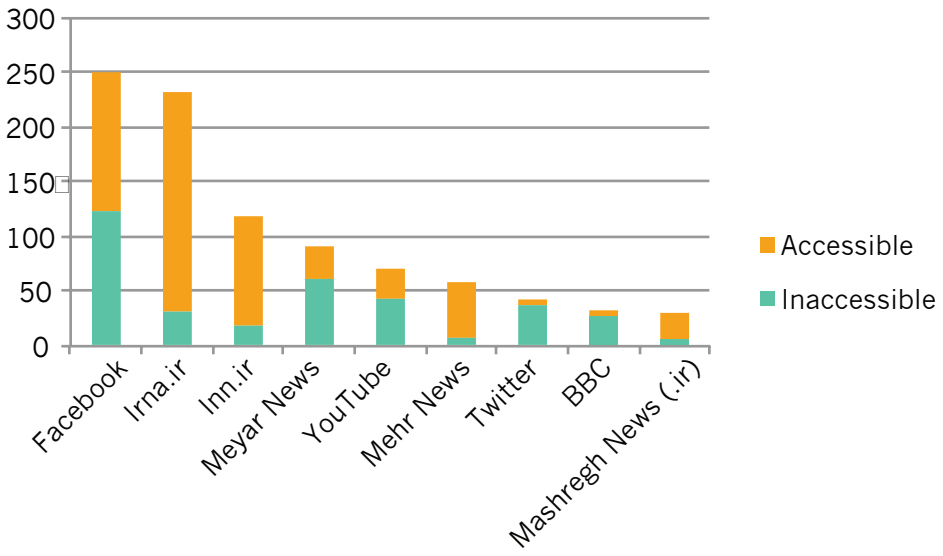


Figure 1: Herdict reports from Iran (select sites): June 1-July 1, 2013

Mohammad Hassan Nami, Iran's Minister of Communications and Information Technology during this period, told Tasnim News Agency that the restrictions on Internet usage were part of "security measures taken to preserve calm in the country during the election period," according to Radio Free Europe.[2] However, Herdict data shows a far broader set of restrictions on freedom of expression online.

Herdict users from Iran reported substantially more inaccessible sites with foreign domains than local .ir sites. Between June 1 and July 1, Herdict received 2,283 accessible reports and 1,250 inaccessible reports from Iran, for an overall inaccessibility rate of 35 percent. Of the 1,250 inaccessible reports, only 73 pertained to sites on the Iranian top-level domain (.ir); the remaining 1,177 inaccessible reports pertained to non-.ir sites (e.g., facebook.com, youtube.com, etc.).

ASL 19 conducted surveys that confirm this data. Their surveys show Iranians experienced more

difficulty with non-.ir websites than with .ir websites. Between June 11 and July 1, 22 percent of survey respondents reported normal access to .ir websites, compared to 6 percent who reported normal access to non-.ir websites. During the same period, 90 percent of Herdict reports about .ir sites indicated those sites were accessible, compared to a 60 percent accessibility rate for non-.ir sites.

Censorship in Iran during this period was neither monolithic nor static, something underscored by looking at some specific sites. Facebook, Twitter, and YouTube are some of the most popular sites in the world, as well as frequent targets of censorship. During the election period, 49, 88, and 61 percent of reports from Iran about these sites, respectively, indicated that they were inaccessible. ASL 19 survey data also showed limited access to these sites.

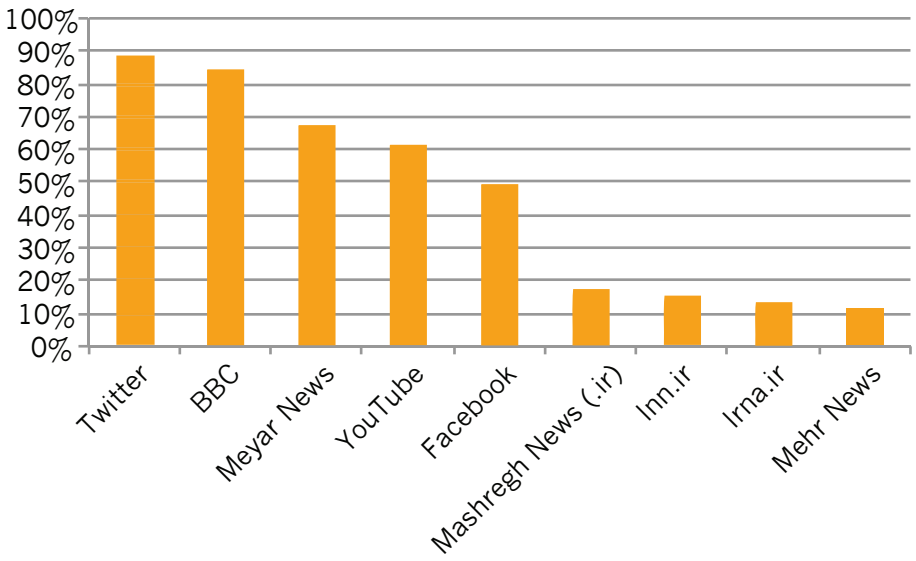


Figure 2: Percentage of Herdict reports indicating site inaccessible in Iran: June 1-July 1, 2013

In the post election period, access appears to have substantially improved. This is particularly true for Iranian news sites. Herdict collected reports about the websites for Farsi News, Gooya News, Iran News Network, Iranian Labour News Agency, Islamic Republic News Agency, Mashregh News, Mehr News, and Meyar News. Immediately following the election, 26 percent of the reports Herdict received about these sites indicated inaccessibility. But just over a week later, this number had dropped to barely over 5 percent.

Immediately following his election, President Hassan Rouhani acknowledged that Internet filtering doesn't work and called social networking sites "a welcome phenomenon." Whether this will lead to fundamental changes in the way Iran treats Internet freedom remains to be seen. But this most recent election demonstrates that Iran continues to improve its proficiency at targeted censorship concurrent with major events such as elections and historical anniversaries.

Notes

1. Ronald Diebert and Rafal Rohozinski, "Good for Liberty, Bad for Security? Global Civil Society and the Securitization of the Internet," in Access Denied, ed. Ronald Deibert et al. (Cambridge: MIT Press, 2008), 144
2. Golnaz Esfandiari, "Iran Admits Throttling Internet To 'Preserve Calm' During Election," Radio Free Europe/Radio Liberty, June 26, 2013, http://www.rferl.org/content/iran-internet-disruptions-election/25028696.html.

CHINA MOVES TO THE CLOUD

Mark Wu

China may be home to the most Internet users in the world and increasingly sophisticated Internet companies, but when it comes to unleashing the potential of cloud computing, China lags behind. Industry analysts estimate that China currently accounts for only 3 percent of the global cloud computing market.[1] In the 2013 Global Cloud Computing Report, China placed 19th out of 24 countries in terms of the conduciveness of its policy environment for cloud computing.[2] Realizing the importance of this emergent technology and not wishing to be left behind, China is in the midst of an aggressive push to expand its cloud computing infrastructure and services. This initiative involves a mixture of government and private efforts. All of these efforts, however, are constrained by political and economic considerations that will likely result in Chinese "clouds" being unique, rather than fully integrated with the rest of world.

The importance of cloud computing to the Chinese government is reflected by its listing as one of seven priority areas in the government's Twelfth Five-Year Plan (2011-15). In November 2011, the National Development and Reform Commission (NDRC), along with the Ministry of Industry and Information Technology (MIIT) and the Ministry of Finance, agreed to earmark Rmb 1.5 billion ($245 million) to projects in cloud computing.[3] These projects are being aided by significant government investments in the development of data centers around the country and are being overseen by an NDRC expert committee tasked with guiding the development of the Chinese cloud computing industry.[4]

The central government is developing cloud computing pilot programs in several cities with varied areas of focus. For example, the Beijing Harmony Cloud Project (北京祥云计划) focuses on developing infrastructure-as-a-service, as well as cloud applications in storage and search; the Shanghai Cloud Sea Project (上海云海计划) targets small business, financial services, healthcare, and media services.[5] In other areas, from Guangzhou to Chongqing, local governments are offering their own incentives—ranging from land grants to special tax benefits—to attract cloud computing industry investment.

Beyond serving as a policy coordinator, the government itself is an active user of cloud technology. Its rapid adoption of cloud services is driven by its dual interests in increasing workplace efficiency and providing a jump-start to the industry. In addition to e-government initiatives, the state is likely to promote the adoption of cloud-based solutions in health care and education, as well as possible cloud initiatives in several industries dominated by state-owned enterprises such as petrochemical, telecommunications, and electricity.[6]

Despite these many domestic initiatives, foreign companies hoping to tap into China's burgeoning market face a number of regulatory restrictions. This includes limitations on foreign investment in telecommunications and value-added services that effectively require multinationals to engage in joint ventures with Chinese partners. Furthermore, foreign companies must comply with Chinese regulations on content controls, encryption, and state secrets.[7]

Leading foreign cloud providers are taking different approaches to Chinese restrictions. IBM opened a cloud computing center in Beijing as early as 2008 and has engaged in multiple joint venture projects, including collaborating with China's Range Technology in the development of Asia's largest cloud computing center in Langfang, Hebei, near Beijing.[8] Intel Capital has invested in a number of

Chinese cloud computing projects and start-ups.[9] And, in March 2012, IT service provider Internet Initiative Japan agreed to a joint venture with China Telecom to build and operate a cloud-computing platform in conjunction with the country's dominant fixed-line provider.[10]

Meanwhile, major Chinese Internet companies are engaged in an aggressive push to expand their own cloud-related offerings. The earliest mover and a widely-acknowledged industry leader is Ali Cloud (also known by its Chinese moniker, Aliyun). Ali Cloud was spun off from the Alibaba Group, China's largest B2B Internet company. It focuses on providing a broad-range of cloud-based services, including email, storage, CRM, sales force management, inventory management, and financial management. Several other leading Chinese Internet companies, including Tencent and Shanda, are also actively engaged in pursuing cloud-oriented initiatives.[11]

Huawei, China's global telecommunications equipment giant, also recently developed Huawei Telco Cloud Solutions and is offering private and public cloud solutions, as well as partnering with several multinationals to offer enterprise-to-enterprise vertical IT solutions. Huawei reports that its cloud solutions are being used by several top telecommunications carriers including China Mobile, China Telecom, Vodafone, and STC. It operates more than 20 cloud data centers globally including the world's largest for China Mobile. [12]

Until recently, two large US public cloud service providers—Amazon and Microsoft—have stood on the sidelines of the Chinese market. But that too is beginning to change as Chinese competitors rapidly attract new users for public cloud services. Microsoft became the first multinational to receive the necessary qualifications to offer public cloud computing services in China.[13] In June 2013, Microsoft began offering its Windows Azure platform in conjunction with 21Vianet, a Chinese data center service provider. Amazon, meanwhile, has made no announcements of any plans to enter the Chinese market.

While multinationals are only beginning to offer public cloud services in China, the country's leading search provider, Baidu, has built up its own public cloud offering at an astonishing speed. Baidu Cloud provides online storage of photos, contacts, and notes. Like Google, Baidu is hoping that its leadership in search, as well as a comprehensive range of other offerings, from music streaming to word processing, will drive everyday users to its cloud. Baidu Cloud is growing at a rate of 200,000 new users per day, expanding from 20 million users in late 2012 to over 70 million by mid-2013.[14]

Despite the recent aggressive push, cloud computing in China faces four major challenges. These include gaps in the Chinese cloud computing ecosystem, user adoption concerns, lagging tools for cloud management, and regulatory limitations. Developments in each of these fronts are worth monitoring for anyone concerned with the future of cloud computing in China.

In terms of a comprehensive ecosystem to support cloud computing, recent Chinese government initiatives are serving to alleviate hardware infrastructure problems. But hardware alone is insufficient. A robust cloud computing offering also requires a multitude of software to cover interfaces with different consumer segments as well as middleware. Chinese government policies have emphasized open source solutions, but some companies are also developing proprietary tools. In addition, the success of IBM and others outside of China has been due, in part, to robust systems integration (SI) services that assist in the creation of cloud-based solutions for users. SI providers with a deep understanding of cloud-based tools are only just starting to emerge in China. Lastly, while China has wide broadband penetration, download speeds in many parts of the country remain slow. These elements of the

ecosystem require further development to avoid creating bottlenecks in the cloud industry's evolution.

Adoption of cloud computing may also be hampered by lagging user knowledge and adoption willingness. A survey by Accenture of senior Chinese IT executives in 2010 found them to be well behind their American counterparts in terms of their knowledge and actual use of cloud-based services.[15] Chinese executives expressed deep skepticism of public cloud services, particularly in terms of data security and access by foreign governments.[16] Even those enterprises that have moved to the cloud have preferred to use private, rather than public, cloud solutions.[17] Moreover, Chinese executives appear to be primarily focused on taking advantage of the cloud for process improvement and cost savings, and less interested in cloud-based innovation.[18] Unless these user-related limitations are overcome, they will stifle the development of Chinese players into genuine world-class innovators, particularly with respect to public cloud services.

Consumer confidence in cloud-based solutions also depends on the availability of robust cloud management tools. Users need to be assured of the reliability of providers' capabilities in terms of managing data across data centers, ensuring disaster recovery, protecting privacy, tailoring intelligent services, etc. On these fronts, China's domestic players still appear to lag behind the more experienced multinationals.[19] Multinationals, however, may be reluctant to share their latest and most sophisticated tools with Chinese joint venture partners in the face of negative past episodes of IP theft and perceptions of inconsistent enforcement. The pace and quality at which Chinese cloud management tools evolve, based on either homegrown solutions or foreign technology transfer, will also impact the growth of the industry.

Finally, regulatory controls present a huge barrier not only to the ability of foreign multinationals to operate in China. They also indirectly hamper the ability of China's domestic players to develop the capacity to expand their homegrown solutions overseas. The Great Firewall and other Chinese governmental controls ensure that much of the world's public cloud solutions will not be easily accessible within China.[20] Meanwhile, China's indigenous cloud solutions will be tailored to Chinese regulatory demands and are likely to be different than those offered elsewhere. This means that despite rapid growth projections, in the medium term, only the few Chinese multinationals with deep resources and extensive experience overseas, such as Huawei, have any potential to develop solutions that can meet Chinese demands and compete internationally with solutions offered by global industry leaders.

Like the rest of the Internet, the cloud will become increasingly Chinese in the coming years. Large investments by the government and private companies are paving the way for faster growth of cloud computing in China and creating significant opportunities for both domestic and international technology firms. Much remains uncertain, however, about how the unique obstacles to Internet innovation in China can be overcome. Until these obstacles are dealt with, the greatest likelihood is that China will remain a fast follower, albeit a critically important one, rather than a genuine global leader in cloud computing.

Notes

1. Xath Cruz, "The State of Cloud Computing Around the World: China," Cloud Times, October 1, 2012, http://cloudtimes.org/2012/10/01/cloud-computing-world-china/.
2. Business Software Alliance, 2013 BSA Global Cloud Computing Scorecard: A Clear Path to Progress, http://cloudscorecard.bsa.org/2013/.
3. Han Zhang, "China Sets Out Cloud Computing Strategy – The Cloud China 2013 Exhibition and Seminar," HKTDC Research, May 8, 2013, http://economists-pick-research.hktdc.com/business-news/article/International-Market-News/China-sets-out-cloud-computing-strategy-The-Cloud-China-2013-Exhibition-and-Seminar/imn/en/1/1X000000/1X09SWXF.htm; Wai-Ming To et al., "Cloud

Computing in China: Barriers and Potential," IT Pro 15, no. 3 (2013): 48-53.
4. US Information Technology Office, "China's Cloud Computing Policies and Implications for Foreign Industry," November 2012, http://cryptome.org/2012/12/usito-china-cloud.pdf.
5. Ibid.; Jackson He et al., "China: A Booming Market for Cloud Computing," Intel Technology Journal 16, no. 4, (2012): 27, http://www.intel.com/content/dam/www/public/apac/xa/en/pdfs/ssg/China-A_Booming_Market_for_Cloud_Computing_eng.pdf.
6. Cruz, "The State of Cloud Computing."; Penny Jones, "China's Growing Cloud Industry," Datacenter Dynamics, May 21, 2012, http://www.datacenterdynamics.com/focus/archive/2012/05/china%E2%80%99s-growing-cloud-industry.
7. For further details see, e.g., Rocky Lee, "Cloud Computing in China: Implications of a Complex Environment," Cadwalader, Wickersham & Taft LLP, Clients & Friends Memo, July 11, 2012, http://www.cadwalader.com/uploads/cfmemos/0245600eab7512cdcdb269594a040abb.pdf; Agnes L. Liu and Andrew McGinty, "The Hazy Cloud: Legal Challenges for Delivering Cloud Computing in China," Hogan Lovells, September 2, 2011, http://www.lexology.com/library/detail.aspx?g=617313de-59a9-4c6b-8351-9414615e54d6; Jingzhou Tao & Gregory Louvel, "Latest Trends in Cloud Computing in China," Dechert LLP Special Alert, June 2012, http://www.dechert.com/files/Publication/6575ba45-0133-4f6c-a666-8de51a428d64/Presentation/PublicationAttachment/eabd7bcf-a3ba-4257-9a5a-952ad32db05b/Data_Protection_and_Privacy_06-12_Latest_Trends_in_Cloud_Computing.pdf.
8. Julie Zhu, "Langfang: China's Cloud Computing Hub," Financial Times, May 15, 2013.
9. Nir Kshetri, "Diffusion and Effects of Cloud Computing in China: Economic and Institutional Considerations," Pacific Telecommunications Council 2013 Proceedings, http://www.ptc.org/ptc13/images/papers/upload/PTC13_Kshetri_Nir_Paper.pdf.
10. Bien Perez, "Japanese and China Telecom in Cloud Pact," South China Morning Post, March 13, 2012, http://www.scmp.com/article/995327/japanese-and-china-telecom-cloud-pact.
11. Laura Luo, "Company Profile: China's Tencent," Datacenter Dynamics, Aug. 2, 2012, http://www.datacenterdynamics.com/focus/archive/2012/08/company-profile-china%E2%80%99s-tencent; Ben Chiang, "Shanda Publicly Testing Its Cloud Offerings," TechNode, July 23, 2011, http://technode.com/2011/07/23/shanda-publicly-testing-it%E2%80%99s-cloud-offerings/. Tencent's revamped Weiyun (Micro Cloud) offering provides cloud storage, photo storage, Wi-fi hotspot file transfer, and cross-device clipboard features. For more details, see Josh Ong, "Tencent Revamps Cloud Service Weiyun, the Third Prong of Its Mobile Platform," TheNextWeb, September 17, 2012, http://thenextweb.com/asia/2012/09/17/chinas-tencent-building-mobile-lifestyle-weixin-weibo-now-weiyun/.
12. For more information see "Cloud Computing," Huawei website, http://www.huawei.com/en/solutions/arpu-up/hw-001249.htm#.UIXcgmSifWo.
13. Bien Perez, "Microsoft to Promote Cloud Computing in China," South China Morning Post, June 29, 2013, http://www.scmp.com/business/companies/article/1271351/microsoft-promote-cloud-computing-china.
14. C. Cluster, "Baidu Cloud Breaks 70 Million Users, Growing at 200k Users a Day," Tech in Asia, June 27, 2013, http://www.techinasia.com/baidu-cloud-breaks-70-million-users-growing-200k-users-day/.
15. Allan E. Alter et al., China's Pragmatic Path to Cloud Computing, Research Report of Accenture and the Chinese Institute of Electronics, May 2010, http://www.chinacloud.cn/download/ppt/Allan.pdf.
16. While security is the main concern around the world, the Accenture survey found security worries to be stronger in China than in any other country around the world. Chinese executives are particularly worried that the data could be stolen by hackers or accidentally released to other customers of a cloud provider or to the wrong employee. Ibid., 17.
17. Liau Yun Qing, "China Cloud Deployment Dampened by Nascent Enterprise Demand," ZDNet, March 15, 2013, http://www.zdnet.com/cn/chinas-cloud-deployment-dampened-by-nascent-enterprise-demand-7000012662/.
18. See Alter et al., 12.
19. See He et al., 31.
20. See Kshetri, 10.

DATA PRIVACY REFORM IN THE EUROPEAN UNION

Viktor Mayer-Schönberger

In the midst of continuing privacy tussles, such as over Facebook's and Google's privacy policies, and somewhat unexpected new challenges, such as the PRISM and TEMPORA revelations, arguably the most important legislative activity in the privacy field this past year unfolded in the European Union.

Almost two decades ago, and before the Internet became popular, the European Union put in place comprehensive data protection and privacy legislation, the so-called data protection directive. It was the result of years of intense negotiations and mandated that EU member states implement a high level of privacy protection as laid out in the directive by passing appropriate national laws covering data processing of personal information in both the public and the private sector.

In the wake of the Internet's meteoric rise to permeate almost all areas of life, and with social networking platforms and mobile smartphones turning into mass phenomena, the European Commission put forward a plan to update the EU's privacy framework and bring it into the 21st century. To that end, in late 2011 the Commission circulated a new draft privacy regulation, to be enacted by the European Union.

This draft regulation is an evolution of the directive, but it also breaks with the past, both structurally and substantively. Structurally, as a regulation it would become directly applicable law in the European Union rather than (as the directive) needing to be implemented through national legislation. This would mean that implementation differences that to an extent have plagued the European privacy framework would disappear (although enforcement differences might continue). Substantively, the draft includes four innovations: (1) a "right to be forgotten"; (2) a right of data portability; (3) data breach notification requirements; and (4) an increased role for accountability—all paired with more stringent enforcement that includes drastically higher fines for breaches.

While touted by the Commission as a complete overhaul of the privacy framework that meets not simply present but also future privacy challenges, the draft is relatively conservative. Some of its "novel" elements already exist in some form in the existing directive, and were merely expanded (and rebranded). This can be seen both as an advantage (because at its core it signals continuity) and as a disadvantage (because it may be an insufficient reaction to changing times). Expectedly given its prominence, the draft was heavily criticized by stakeholders, who alternately argued that it went either too far or not far enough.

In 2012, intense discussion over the Commission draft ensued in Brussels and throughout Europe. The European Parliament held hearings, and both the European Parliament and the European Council (who must formally vote for such a regulation to be enacted) put forward their own drafts. These clarified the "right to be forgotten" and redirected the data portability right, while data breach duties and enforcement actions were watered down to make them more palatable to industry.

Significant differences in opinion on details persist between Commission, Council, and Parliament, with the Commission aiming to get a regulation passed as soon as possible, the Council somewhat reluctant, and the Parliament arguing for a pragmatic, yet effective measure protecting citizens. The

next twelve months will likely be crucial in whether and what regulation will protect the privacy in Europe in the years to come.

Additional Reading

European Commission, Data Protection: Newsroom, http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm.

THE INFORMATION TECHNOLOGY ACT AND INTERMEDIARY LIABILITY IN INDIA

Christopher T. Bavitz and Bryan Han

Introduction

India's Information Technology Act (the "IT Act"), enacted in 2000, covers several aspects of online and new media technologies in the country, including the security of electronic records and digital signature certificates.[1] In 2008, the IT Act was amended to allow for broad government control and authority over the Internet in many circumstances.[2]

Three features of the amended Act are particularly worthy of note. First, the Act contains provisions that allow for government blocking of websites. Second, provisions in the IT Act (and analogous provisions in India's Copyright Act) provide for "safe harbors" available to online intermediaries. And, third, the Act creates several computer-related criminal offenses that directly relate to online speech and the ability of Internet users to engage in free expression.

Government Blocking of Websites

Under Section 69A of the IT (Amendment) Act, the government is allowed to block access of information through any computer resource if it "is satisfied it is necessary or expedient so to do, in the interest of the sovereignty or integrity of India, defense of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offense." Section 69 also allows the government to intercept, monitor, or decrypt any computer resource for the reasons outlined in § 69A, or to investigate a criminal offense. Section 69B allows the government to monitor and collect any information in order to enhance cyber security or prevent the spread of a computer virus. The government has relied on the IT Act's broad provisions to take sweeping action, disabling access to online content deemed to be of concern. In the summer of 2012, fake videos of Muslims being tortured and promising retaliation—allegedly posted online by radical groups in Pakistan—led to clashes between Muslims and migrant workers from the northeastern state of Assam, causing a massive exodus of Assamese from other parts of the country. In response, the Indian Telecommunications Ministry ordered ISPs and intermediaries to block access to around 300 websites and threatened legal action against those who did not comply.[3] These sites included legitimate news organizations such as ABC and Al Jazeera, as well as social media sites such as Facebook, Twitter, and Google. Social networking sites complied with the governments' orders, while ABC issued a statement saying it was "surprised by the action."[4] A report by Pranesh Prakash of The Centre for Internet & Society noted many technical errors and inconsistencies in list of blocked sites and questioned the effectiveness of the government's efforts.[5]

Safe Harbors

Section 79 of the Act outlines liability for intermediaries hosting content that may violate India's laws. To qualify as an intermediary under the IT Act, a website must either (1) function only to provide access to a communication system over which information made available by third parties is transmitted or temporarily hosted; or (2) not initiate, select the receiver of, or select or modify

the information contained in transmissions by users. Intermediaries are not liable for third-party information, data, or communication links they host. They lose this immunity, however, if they conspire, aid, or abet the commission of an unlawful act, or if they fail to remove material that violates the law after receiving notification from the government or "actual knowledge" from any source that the material is being used to commit an unlawful act.

Guidelines issued by the Ministry of Communications and Information Technology in April 2011 limited the scope of the safe harbor, requiring intermediaries to prevent access to objectionable content across a broadly defined range of content if requested by a public official or private individual. This includes material that is "grossly harmful, harassing, blasphemous," "hateful, or racially, ethnically objectionable, disparaging," "communicates any information which is grossly offensive or menacing in nature," "threatens the unity, integrity, defense, security or sovereignty of India, friendly relations with foreign states," or "is insulting any other nation."[6]

Courts in India have interpreted the IT Act to not cover alleged copyright or patent infringement.[7] In June 2012, amendments to the Copyright Act created a safe harbor provision for websites for copyright infringement. Under § 52(1)(c) of the Copyright Act as amended, "transient or incidental storage" of a work, where the links, access, or integration have not been expressly prohibited by the right holder, is not copyright infringement unless the person responsible for the copy has reasonable grounds for believing it is copyright infringement.[8]

Criminal Liability

Section 66A of the amended IT Act extends criminal liability beyond receipt of stolen computer resources, identity theft, cheating by impersonation, violation of privacy, cyberterrorism, obscenity, and child pornography to cover the sending of offensive messages through a communications service. A person is criminally liable for sending, via computer, "any information that is grossly offensive or has menacing character," information the sender knows to be false "for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will," or electronic messages sent "for the purpose of causing annoyance or inconvenience, or to deceive or mislead the recipient about the origin of such messages." In response to public outcry against arrests made under §66A, the government issued a directive on January 9, 2013, requiring prior approval by senior police officials before making arrests.[9]

Additional Reading

Vikas Baijaj, "India Puts Tight Leash on Internet Free Speech," New York Times, April 27, 2011, http://www.nytimes.com/2011/04/28/technology/28internet.html.

Department of Electronics and Information Technology, Ministry of Communications Technology, Government of India, Cyber Security Strategy: Overview, http://deity.gov.in/content/overview.

Department of Electronics and Information Technology, Ministry of Communications Technology, Government of India, Cyber Security Strategy: Current Scenario, http://deity.gov.in/content/current-

scenario.

Manoj Mitta, "Lessons from UK on misuse of Section 66A," The Times of India, December 1, 2012, http://articles.timesofindia.indiatimes.com/2012-12-01/india/35530325_1_section-66a-facebook-post-lords.

United States Library of Congress, Country Profile: India (December 2004), available at http://lcweb2.loc.gov/frd/cs/profiles/India.pdf.

Notes

1. The Information Technology Act (2000), available at http://deity.gov.in/sites/upload_files/dit/files/downloads/itact2000/itbill2000.pdf (last visited: August 7, 2013).
2. The IT (Amendment) Act (2008), available at http://deity.gov.in/sites/upload_files/dit/files/downloads/itact2000/it_amendment_act2008.pdf (last visited: August 7, 2013).
3. Gianluca Mezzofiore, "India Blocks Website Pages for 'Spreading Fear' over Assam Violence," International Business Times, August 24, 2012, http://www.ibtimes.co.uk/articles/377157/20120824/india-blocks-more-300-internet-pages-news.htm. See also ET Bureau, "Assam violence: Cyber war continues, government blocks 89 more web pages to avoid panic," The Economic Times, August 21, 2012, http://articles.economictimes.indiatimes.com/2012-08-21/news/33302897_1_inflammatory-content-government-blocks-home-ministry.
4. Simon Roughneen, "India Blocks Facebook, Twitter, Mass Texts in Response to Unrest," PBS MediaShift, August 28, 2012, http://www.pbs.org/mediashift/2012/08/india-blocks-facebook-twitter-mass-texts-in-response-to-unrest241.
5. Pranesh Prakash, "Analysing Latest List of Blocked Sites (Communalism & Rioting Edition)," The Centre for Internet & Society, August 22, 2012, http://cis-india.org/internet-governance/blog/analysing-blocked-sites-riots-communalism. See also Vikas Bajaj, "Internet Analysts Question India's Efforts to Stem Panic," New York Times, August 21, 2012, http://www.nytimes.com/2012/08/22/business/global/internet-analysts-question-indias-efforts-to-stem-panic.html.
6. Information Technology (Intermediaries Guidelines) Rules (2011), available at http://deity.gov.in/sites/upload_files/dit/files/GSR314E_10511(1).pdf.
7. See Super Cassetes Industries, CS No. 2682/2008 (Delhi H.C. Jul. 29, 2011), http://www.indiankanoon.org/doc/216257/.
8. The Copyright (Amendment) Act (2012) § 52(1)(c), http://www.copyright.gov.in/Documents/CRACT_AMNDMNT_2012.pdf.
9. Government of India/Bharat Sarkar, Department of Electronics and Information Technology, "Advisory on Implementation of Section 66A of the Information Technology Act, 2000," No. 11(6)/2012-CLFE, January 9, 2013, http://deity.gov.in/sites/upload_files/dit/files/Advisoryonsection.pdf.

INDIA'S IDENTITY CRISIS

Malavika Jayaram

India's Unique Identity (UID) project is already the world's largest biometrics identity program, and it is still growing. Almost 530 million people have been registered in the project database, which collects all ten fingerprints, iris scans of both eyes, a photograph, and demographic information for each registrant. Supporters of the project tout the UID as a societal game changer. The extensive biometric information collected, they argue, will establish the uniqueness of each individual, eliminate fraud, and provide the identity infrastructure needed to develop solutions for a range of problems. Despite these potential benefits, however, critical concerns remain about the UID's legal and physical architecture as well as about unforeseen risks associated with the linking and analysis of personal data.

The most basic concerns regarding the UID project stem from the fact that biometric technologies have never been tested on such a large population. As a result, well-founded concerns exist around scalability, false acceptance and rejection rates, and the project's core premise that biometrics can uniquely and unambiguously identify people in a foolproof manner. Some of these concerns are based on technical issues—collecting fingerprints and iris scans "in the field," for instance, can be complicated when a registrant's fingerprints are eroded by manual labor or her irises are affected by malnutrition and cataracts. Other concerns relate to the project's federated implementation architecture, which, by outsourcing collection to a massive group of private and public registrars and operators, increases the chance for data breaches, error, and fraud.

Perhaps even more vexing are concerns regarding how the UID, which promises financial inclusion (by reducing the identification barriers to opening bank accounts, for example), might in fact lead to new types of exclusion for already marginalized groups. Members of the LGBT community, for instance, question whether the inclusion of the transgender category within the UID scheme is a laudable attempt at inclusion, or a new means of listing and targeting members of their community for exclusion. More fundamentally, as more and more services and benefits are linked to the UID, the project threatens to exclude all those who cannot or will not participate in the scheme due to logistical failures or philosophical objections.

It is worth noting that the UID is not the only large data project in India. A slew of "Big Brother" projects exist: the Centralised Monitoring System (CMS), the Telephone Call Interception System (TCIS), the National Population Register (NPR), the Crime and Criminal Tracking Network and Systems (CCTNS), and the National Intelligence Grid (NATGRID), which is working to aggregate up to 21 different databases relating to tax, rail and air travel, credit card transactions, immigration, and other domains. The UID is intended to serve as a common identifier across these databases, creating a massive surveillance state. It also facilitates an ecosystem where access to goods and services, from government subsidies to drivers' licenses to mobile phones to cooking gas, increasingly requires biometric authentication.

The UID project was originally vaunted as voluntary, but the inexorable slippery slope toward compulsory participation has triggered a series of lawsuits challenging the legality of forced enrollment and the constitutionality of the entire project. Most recently, in September 2013, India's federal Supreme Court affirmed by way of an interim decision that the UID was not mandatory, that not possessing a UID should not disadvantage anybody, and that citizenship should be ascertained as

a criteria for registering in order to ensure that UIDs are not issued to illegal immigrants. This last stipulation is particularly thorny given that the Unique Identification Authority of India (UIDAI, the body in charge of the UID project) has consistently distanced the UID from questions of citizenship under the justification that it is a matter beyond their remit (i.e., the UID is open to residents, and is not linked to citizenship). The government moved quickly to urge a modification of the order, but the Supreme Court declined to do so and will instead release its final decision after it reviews a batch of petitions from activists and others. The UIDAI approached the court, arguing that not making the UID mandatory has serious consequences for welfare schemes, but the court recently ordered the federal government, the Reserve Bank of India, and the Election Commission to delink the LPG cooking gas scheme from the UID. This is a considerable setback for the project, given that this was one of the most hyped linkages for the UID. It remains to be seen whether the court will similarly halt other attempts to make the UID mandatory.

In the meantime, the UID project is effectively being implemented in a legal vacuum without support from the Supreme Court or Parliament. The Cabinet is seeking to rectify this and has cleared a bill that would finally provide legal backing for the UID program—its previous attempt was rejected by the Standing Committee on Finance in 2010. This bill is scheduled to come up for debate during the winter session of Parliament. The bill's progress, along with the final decision of the Supreme Court, will have far reaching consequences for the UID project's implementation and longevity, as well as for the relationship between India's citizens and the state.

If fully implemented, the UID system will fundamentally alter the way in which citizens interact with the government by creating a centrally controlled, technology-based standard that mediates access to social services and benefits, financial systems, telecommunications, and governance. It will undoubtedly also have implications for how citizens relate to private sector entities, on which the UID rests and which have their own vested interests in the data. The success or failure of the UID represents a critical moment for India. Whatever course the country takes, its decision to travel further toward or turn away from becoming a "database nation" will have implications for democracy, free speech, and economic justice within its own borders and also in the many neighboring countries that look to it as a technological standard bearer.

The Indian government seems to envision "big data" as a panacea for fraud, corruption, and abuse, but it has given little attention to understanding and addressing the fraud, corruption, and abuse that massive databases can themselves engender. The government's actions have yet to demonstrate an appreciation for the fact that the matrix of identity and surveillance schemes it has implemented can create a privacy-invading technology layer that is not only a barrier to online activity but also to social participation writ large.

The lack of identification documents for a large portion of the Indian population does need to be addressed. Whether the UID project is the best means to do this—whether it has the right architecture and design, whether it can succeed without an overhaul of several other failures of governmental institutions, and whether fixing the identity piece alone causes more harm than good—should be the subject of intense debate and scrutiny. Only through rigorous threat modeling and analysis of the risks arising out of this burgeoning "data industrial complex" can steps be taken to stem the potential repercussions of the project not just for identity management, fraud, corruption, distributive justice, and welfare generally, but also for autonomy, openness, and democracy.

MARCO CIVIL: A BILL REGULATING NET NEUTRALITY AND CIVIL RIGHTS ONLINE IN BRAZIL

Ronaldo Lemos

In June 2013, millions of Brazilians took to the streets to protest for better public services, political reform, and the end of corruption. These protesters shared a desire for more public participation in public life and demanded that the voices of discontent, including those expressed online, be taken into account by decision makers in government.

Years before, the drafting process for the "Marco Civil," a bill of rights for the Internet in Brazil, had put into practice many of these aspirations. In 2009, the Ministry of Justice and the Center for Technology and Society at the FGV Law School in Rio de Janeiro launched an online platform on which anyone could participate in the drafting of the "Marco Civil da Internet."[1] The initiative emerged after widespread public reaction to proposed reforms to the Cybercrime Bill, put forth in 2007. The proposed bill was an attempt to bring Brazilian law in line with existing international norms, including the Convention on Cybercrime.[2] However, like the American bills SOPA and PIPA, it used what some saw as overly broad language to criminalize the free flow of users and information online.

The bill was lambasted in an online petition signed by prominent regional academics for "violat[ing] the freedom, creativity, privacy, and dissemination of knowledge in the Brazilian Internet."[3] Brazilian President Dilma Rousseff, in an address to the International Forum for Free Software, voiced her opposition as well, stating that the proposal "doesn't aim to fix the abuse of the Internet. It really tries to impose censorship."[4] A modified version of the bill was approved by Brazil's Senate in 2008 but languished in the House of Representatives, where it was ultimately vetoed in 2012.[5]

The Marco Civil draft grew out of more than 800 initial contributions made via the online platform and via email. Successive drafts were debated online and at multiple public hearings.[6] The draft of the Marco Civil, thanks to public participation, embraced a remarkable set of rights. Issues covered include net neutrality, privacy, freedom of expression, safe harbors for intermediaries, open government, and limitations on the retention, and access to user data. The Executive Government approved the draft, and President Rousseff sent it to Congress in August 2011.

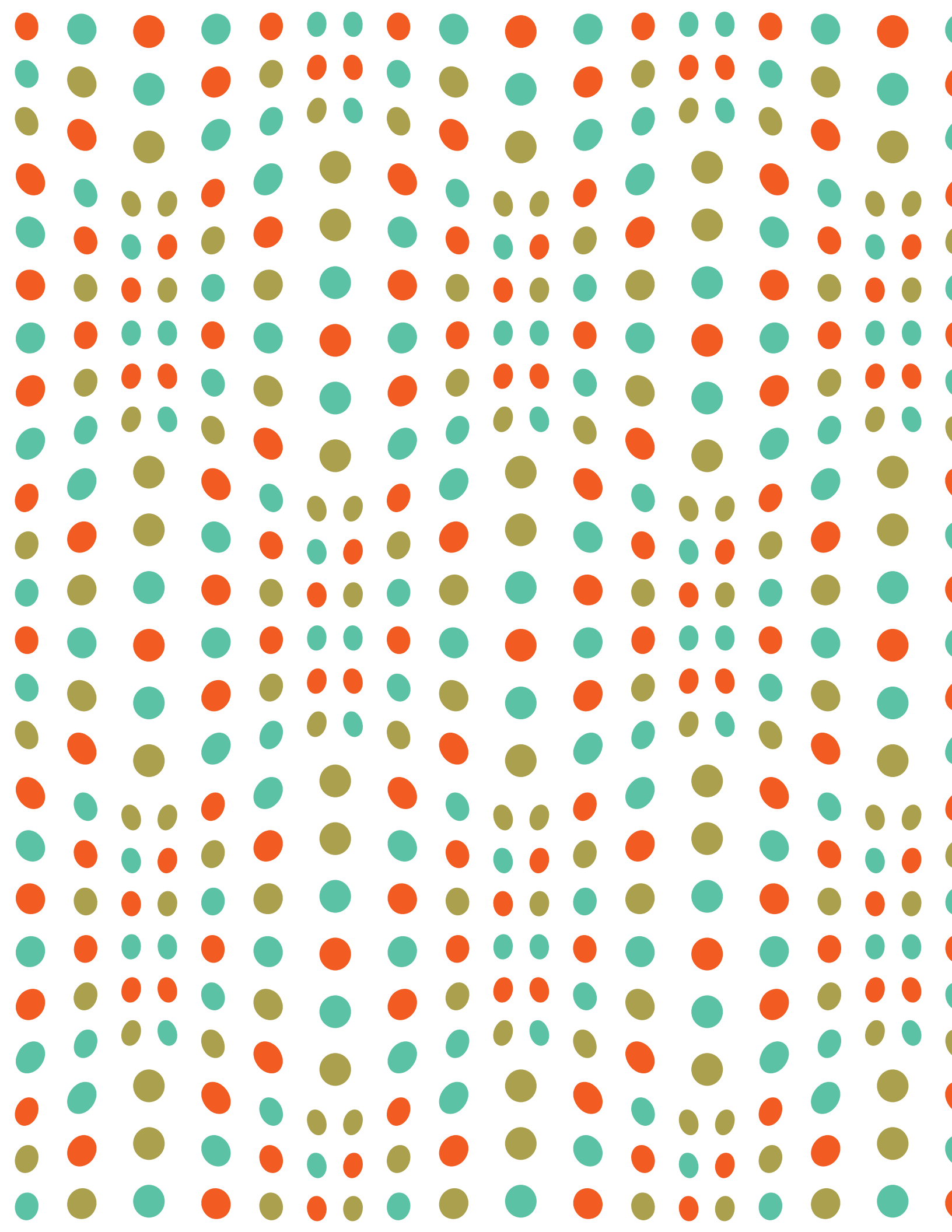
The Marco Civil was scheduled to be voted on several times in late 2012, but pressure from telecommunications companies, which are not happy with the net neutrality and privacy provisions, has delayed the vote.

The bill remained in limbo through the first half of 2013, but Edward Snowden's allegations have tilted the game. President Rousseff strongly condemned the revelations of NSA surveillance activities and renewed pressure on Congress to approve the Marco Civil as quickly as possible. The government also introduced a highly criticized amendment into the draft bill: a new provision that mandates that data collected locally about Brazilian citizens or companies must be stored in Brazil.[7] If approved, global Internet companies will have to maintain datacenters in the country. The proposed amendment, as expected, has stirred quite a lot controversy and is currently being widely debated.

The importance of the Marco Civil should not be underestimated. The lack of specific Internet laws, which has been the case in Brazil for many years, does not necessarily lead to greater online freedom, but to a high level of legal uncertainty, contradictory court decisions, and threats to privacy. If approved in its original draft, Marco Civil will be an example of a positive, rights-enabling legislation, capable of influencing other countries.

Notes

1. Marco Civil da Internet, http://www.culturadigital.br/marcocivil.
2. Paulo Rena, "AI5-Digital 2007/2008: os últimos 12 meses da tramitação no Senado Federal," Hiperfície, June 28, 2011, http://hiperficie.wordpress.com/2011/06/28/ai5-digital-20072008-os-ultimos-12-meses-da-tramitacao-no-senado-federal/.
3. "Veto by the project cybercrimes - In defense of liberty and the progress of knowledge in the Brazilian Internet," http://www.petitiononline.com/veto2008/petition.html.
4. "President of Brazil's Address to FISL 2009," Electronic Frontier Foundation, https://www.eff.org/issues/cybercrime/president-brazil-2009.
5. "PL 84/1999," http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=15028.
6. "Marco Civil: Support the Brazilian Internet principles and multistakeholder legislative model," November 9, 2012, Marco Civil da Internet, http://marcocivil.com.br/en/marco-civil-threatened/.
7. Brian Winter, "Brazil's Rousseff targets internet companies after NSA spying," Reuters, September 13, 2013, http://in.reuters.com/article/2013/09/12/usa-security-snowden-brazil-idINDEE98B0GF20130912.



COMPANIES AS ACTORS

Robert Faris and Urs Gasser

Companies form the functional core of the Internet. The private sector owns a vast proportion of the physical infrastructure, produces the hardware and software that light up the network, develops innovative services and applications, acts as gateways for residential and business access to the Internet, and hosts the lion's share of content and information. Companies act as merchants, aggregate data and knowledge, serve as media outlets, and house the data and networks that digitally link communities around the globe. In contrast to the pre-Internet commercial world, a prime source of value for much of this activity is based on promoting and leveraging the pro-social urges and voluntary participation of users.

> ***Bringing together companies, rights advocates, investors, and academics to collectively defend against government overreach and advance international human rights standards, GNI aspired to responsible company decision making, collaborative learning, and policy engagement.***
>
> —COLIN M. MACLAY
> Dilemmas and Dialogue: GNI and the Transborder Internet

And while the constellation of businesses that participate in the Internet economy is vast and diverse, a modest number of very large firms dominate the action. Much, if not all, of this can be explained by economies of scale and network effects. Internet enterprises are bolstered by scale. For social networks, search algorithms, social media, content aggregation, advertising, physical infrastructure, and hardware and software development, there are inherent self-reinforcing advantages to being big. And with size comes power, responsibility, and scrutiny. Private companies are caught up in the midst of the most challenging and consequential policy questions facing the Internet: freedom of expression, privacy, surveillance, security, civil liberties online, net neutrality, access to broadband, cybercrime, and law enforcement. As the intermediaries between individuals, civil society, governments, and other companies, technology companies not only provide the playing field but are increasingly being called upon to referee the match. In countries that filter the Internet, ISPs are enlisted to implement the blocking. When governments seek information on Internet users, whether for legitimate law enforcement or to pursue political opposition, they turn to ISPs, cell phone carriers, social media platforms, and content hosts. And when civil society feels that online liberties, privacy protections, and security are not being upheld, they lobby the companies; at times with the support of sympathetic governments and at times demanding that companies provide a layer of protection from governments that are seen as predatory.

While there are segments of the Internet operated by public and non-profit entities—for example municipally-owned networks, government infrastructure, and systems run by schools and universities—these comprise a small portion of Internet traffic. A majority of Internet capacity and data flows are sustained by private owners and operators, and are shaped and maintained by a small number of commercial business models.

Subscription-based models support ISPs that connect businesses and residences to the Internet, as well as commercial software and many media and entertainment services, including news sites (e.g., the New York Times and Wall Street Journal) and video distributors (e.g., Netflix and digital access to cable channels). Online sales of merchandise, for example through Amazon and eBay, constitute a different model. A third model based on advertising revenue supports search engines, a wide range of online media, social media platforms, and other online content hosting services, including many of the biggest players (e.g., Google/YouTube, Yahoo!, Facebook, and Twitter).

While these business models are structurally different, they all rely on access to important personal data about their users. Data collection, aggregation, analysis, and sale is a key part of many companies' value proposition, whether to sell the data to other companies, to increase advertising revenue by better targeting of advertisements, or to provide better services to their customers. These business models, supported by user data and economies of scale, have combined to fuel the rapid growth of the Internet and the many benefits of digital activity, and in doing have also contributed to the tensions and unresolved conflicts that have arisen related to privacy, surveillance, security, and freedom of expression. In each of these areas, companies are brought into the fray. As intermediaries between governments and citizens, and between citizens and citizens, technology companies are drawn into serving several, sometimes competing functions: cooperating with law enforcement, protecting users against security breaches and the excessive prying by governments and others, and setting behavioral and content standards on their platforms (in effect creating their own laws).

In the realm of privacy, persistent unresolved tensions exist between website hosts, social media and social networking companies, and their users. This stems from data that is willingly shared by users—their location; love life; preferences in film, music, or food; and so on—and information that is gathered surreptitiously, for example by quietly tracking a user's web browsing habits. This jumps into the area of state surveillance when governments come looking for this same data. For governments, the cooperation of companies in pursuing criminal activity online is instrumental in their ability to govern digital activity. Companies then find themselves in the awkward position of balancing user privacy against the demands of law enforcement agents. For technology companies that live or die based on the continued participation of users, maintaining trust among their user base is critical. Pointing out to users that their privacy information might be shared with the government has never been a popular option for the marketing department. Pretending this doesn't exist is not viable either. A longstanding strategy for some companies has been to restrict cooperation to requests made with clear and specific legal authority. A more recent strategy is to make the entire process more transparent by publishing the type and quantity of law enforcement requests along with company responses.

> ***In 2009, Google published the first transparency report; Twitter followed suit in 2012. Nearly a dozen companies are now releasing transparency reports, with more on the way.***
>
> —RYAN BUDISH
> Transparency Reporting

Companies have been lauded as protectors of free speech when pushing back against government content restrictions, criticized for enacting terms of service agreements that prohibit legally protected speech on their sites, faulted for too easily removing content at the request of others, and condemned

for not going far enough to eliminate harmful speech from their platforms. Given the range and quantity of discussion on these platforms related to matters of political and social relevance, these private companies are acting as hosts for the networked public sphere. This newfound power instilled in intermediaries has the effect of transferring to them authority that has traditionally resided in the judiciary.

> ***As people are moving information previously hidden in locked file cabinets or safes into their personal clouds, companies have inadvertently gained unprecedented power over who can access and control information about individual citizens.***
>
> —DALIA TOPELSON
> The New Guard

In the area of security, most Internet users rely on a handful of technology companies that provide them with connectivity, serve their email, and host their content to also provide them with protection against online attacks, in an arrangement that Bruce Schneier describes as feudal.

Governments will continue to seek more effective control over cyberspace by enlisting help from companies, whether through coercion or voluntary action. A prime example is the makers of filtering and surveillance tools that have stepped forward to sell their products to governments around the world. Another set of smaller companies occupy the opposite end of the spectrum, developing products meant to prevent governments from accessing user information and helping users circumvent filtering.

> ***From the mid-2000s onwards, the Citizen Lab has documented numerous cases of products developed in North America and Europe being used for censorship and surveillance by governments with poor human rights records, and in some cases under international sanctions.***
>
> —RON DEIBERT AND MASASHI CRETE-NISHIHATA
> The Commercialization of Censorship and Surveillance

In this quasi-borderless world, the importance of the physical location of technology companies' personnel and servers is only growing over time. The social media monitoring apparatus of China is made possible only by having direct jurisdiction over the social media companies that do business there. Subject to filtering that prevents building a meaningful share of the market, foreign-hosted competitors are no longer viable alternatives in China. The United States government enjoys a similarly strong position for law enforcement agencies and regulators given the number of influential technology firms based there. Other countries such as India, Iran, and Vietnam have long pushed for greater control over foreign-based platforms that serve their citizens. For companies, this constitutes a momentous decision: whether to risk being shut out of growing markets or forced into making decisions that infringe on the civil liberties of their users.

There are many other contentious issues in the digital world that we do not take up in this report, some of which pit companies against one another. The debate over the future of copyright protections and digital media is far from resolved. Those that rely on the traditional content licensing and distribution industries are in conflict with online platforms that host user generated content and web-native services whose business models are built not on content licensing but rather on search, indexing, and aggregation. The patent wars continue to rage, touching all corners of the Internet and drawing in device and hardware makers as well as retailers, online platforms, software developers, and others. Interoperability is an ongoing concern as companies and governments continue to wrangle over technology standards. Another set of debates revolves around broadband markets and investments in physical infrastructure. In residential markets, entrants argue for access to last mile infrastructure controlled by incumbent telecommunication providers; the net neutrality debates generally divide broadband providers and content distributors.

The privately controlled core of the Internet generally co-exists amicably with the vast and growing stocks of public knowledge and social capital that reside online. This uneasy equilibrium may not last, particularly as political pressures mount for governments to be more proactive in addressing digital matters.

DILEMMAS AND DIALOGUE: GNI AND THE TRANSBORDER INTERNET

Colin M. Maclay

It has been less than a decade since Shi Tao was sentenced to a decade of hard labor by a Chinese court using data from his Yahoo! email account, Michael Ante's blog was deleted based on an informal law enforcement request to a Microsoft joint venture, and Google removed search results in accordance with Chinese law. These developments, which garnered significant public and private attention and concern, formed part of the inspiration to create the Global Network Initiative (GNI), a multi-stakeholder effort to protect and advance online expression and privacy through principles, implementation guidelines, and external accountability measures.

Bringing together companies, rights advocates, investors, and academics to collectively defend against government overreach and advance international human rights standards, GNI aspired to responsible company decision making, collaborative learning, and policy engagement. It promised a valuable complement to legislative solutions, which have made little progress and face challenges not only of jurisdiction, but also in responding to the dynamic nature of technology, companies, users, and governments. Rather than expecting compliance with existing laws, however, true success depended in part on companies actually pushing back against government requests for personal information or content removal—first by mitigating risks, but also by resisting demands by law enforcement in some cases, something no other multi-stakeholder initiative had attempted.

Since the GNI's inception, technology has helped topple governments, connectedness and online activity have skyrocketed, and concerns about privacy and freedom of expression have unfurled and deepened. Pressures on and expectations of companies have increased, and attention to their situation has broadened and mounted. Company reactions have varied, including start-ups embracing and established companies adopting expression and privacy issues as part of their identity (Twitter, Google, Yahoo!), joining GNI (Facebook, LinkedIn), denying any role (Cisco), or even closing their doors (Lavabit, Silent Circle). GNI has become more established and completed its first full round of external company assessments, increased substantially in number and diversity of participants, and is directing significant attention to policy engagement. Notably, it has also generated a significant strain of unofficial problem solving through its robust network.

The most recent revelations about widespread warrantless state surveillance with insufficient oversight have added new dimensions to the conversation, calling the activities of robust democracies into question and increasing concerns about the role of the companies that are core to connectivity, physical infrastructure, access to knowledge, collaborative and social networking platforms, and access to user information. The limitations of standard regulatory models for this inherently trans-jurisdictional medium have been further exposed, demonstrating that extending national legal requirements across borders is hard, whether trying to protect civil liberties in other jurisdictions or to enforce domestic laws on foreign platforms. The result of this regulatory patchwork is that security agencies can gather data that would be otherwise legally inaccessible to them.

The limitations to transparency around government collection of user information and constraints on what companies can disclose exacerbate the challenges to policymakers, users, and advocates to developing an empirical understanding of government and company behavior. In addition to encour-

aging more transparency, GNI has endeavored to compensate for this gap through third-party expert assessments of company processes and their actual practices. The Snowden revelations have added to the challenge of National Security Letters (which include a gag order), sowing frustration and distrust among allies (actual and potential), even as companies and civil society seem to need each other more than ever. Indeed, EFF left GNI in October 2013 citing the inability to carry out a full and honest dialogue given the government constraints on company reporting, an indictment of the legal regime rather than the private sector. In an otherwise forthcoming setting, there is an elephant in the room.

Once the concern of a select (or paranoid) few, privacy is now at the forefront for mainstream users and diverse civil society organizations. Companies are finally improving their own security practices and rethinking—and changing—data collection, transmission, and storage practices. Cloud and other online providers are facing the daunting business implications of user distrust, and governments are exploring nationalization of cloud services, which could either protect their citizens or expose them to even greater risk. Recognizing the fundamental nature of the threat at hand, disparate groups are also working collaboratively for policy reform in coalitions like We Need to Know, which illustrates a range of shared priorities and underscores the benefit of ongoing collaboration across communities. As governments feud (with each other and their citizens) and explore extreme measures (such as the new cloud platform proposal in Brazil), and legislators hold hearings on all sides of the issues, the importance of coalitions is clear. Some feel a palpable risk for Balkanization of the Internet.

While the trajectory of these developments is uncertain, there can be no doubt that that online privacy and free expression are very much at risk globally. NSA and FISA maybe the acronyms of the moment, but other governments are likely to be implicated or to imitate this behavior. Invasive surveillance capabilities are becoming more available and affordable, suggesting wider use and increased oversight challenges (plus a host of non-government surveillance concerns). We are more connected, live more of our lives online, and live them in increasingly interconnected ways, massively increasing the amount and value of information potentially available to prying eyes—and the importance of dealing with that data responsibly from collection to storage, transmission, and disclosure.

In the past, many of the companies who paid the greatest attention to these issues seemed to have been prompted by painful lessons (the telcos remain largely immune to learning, however). Other civic actors blamed the companies for the shortcomings, fairly and not, with incomplete understanding of the issues. It now seems that most parties increasingly understand the dynamic and daunting nature of the challenge before us and the fact that we will continue to need a variety of resources to navigate this terrain, from the law to multi-stakeholder groups like GNI, and technology solutions alongside user norms. From the Internet's inception, bottom-up, multi-sector, participatory standards bodies have played an important role in promoting a robust and vibrant Internet, and, while imperfect, they remain an important part of the tapestry. GNI is a promising approach to developing global standards, advancing good practice, and solving concrete problems around online expression and privacy. With its organizational foundation laid, GNI can (and must) now embody more of that "Internetty" spirit, collaboratively, creatively, and practically taking on these challenges and helping to sustainably protect these human rights, the businesses built atop them, and their potential support for social progress. This is important because everyone can agree that we all need the help in these trying times.

TRANSPARENCY REPORTING

Ryan Budish

A pervasive surveillance apparatus for collecting information about the users of services like Gmail and Facebook. I'm not talking about the NSA and the secret programs that Eric Snowden revealed: in the US, personal data is also collected under the legal and non-secretive Stored Communications Act (SCA), and other countries have their own, similar mechanisms. We don't think of this form of collection as extensive or pervasive because accurate aggregate figures are hard to come by. That needs to change.

The US's SCA is an outdated piece of legislation, passed well before we had high-speed Internet or gigabytes of free cloud storage. It gives law enforcement the ability to collect substantial personal data, often with minimal court supervision. For instance, a law enforcement agency can obtain a person's name, physical address, IP addresses, data about when she signs on and off of an online service, and her payment processing information, simply by issuing a subpoena—a demand for information without court approval. If law enforcement notifies the target of the investigation, it can use a subpoena to collect opened emails of any age and unopened emails stored for longer than 180 days. In some circumstances, notice can be postponed. In other words: a tremendous amount of data is available without any court oversight. And law enforcement can use court orders and warrants to collect even more, if necessary.

What we know about this scale of this data collection comes from transparency reports – disclosures that some companies publish about the requests for user data that they've received from governments. In 2009, Google published the first transparency report; Twitter followed suit in 2012. Over a dozen companies are now releasing transparency reports, with more on the way.

These reports give us some information about the scale of governments' criminal surveillance. For instance, we know that in 2012, US law enforcement agencies made 16,407 requests from Google on 31,072 accounts (not including secret foreign surveillance). When combined with similar data from Twitter and Microsoft, the totals are 28,974 requests on 57,730 accounts.

This is helpful information, but it provides only the faintest glimpse into the full scope of lawful domestic surveillance. The utility of transparency reports as an industry-wide measure is limited by three factors:

Obscured Data: Several transparency reports obscure the amount of domestic surveillance. Facebook and Yahoo!, for example, recently released reports that combine national security requests with domestic criminal requests instead of providing criminal requests as a standalone category. This decision, a concession to the Obama administration in exchange for the right to disclose some data relating to national security requests, diminishes the value of the reports in illuminating either of the surveillance categories.

Inconsistent Data: Even the reports that explicitly provide domestic criminal data differ in some significant ways. For instance, how the companies define critical terms such as "user" or "court order" make the reports difficult to compare and aggregate, leaving us with approximations at best.

Weak Internationalization: Some of the companies releasing reports have provided detailed information about US requests, but none provide the same level about other countries' requests. How many countries use warrants? We can't say because we have only US data.

With more consistency in transparency reporting, we'd be able to develop a more complete picture of the scale of data collection in criminal investigations.

THE NEW GUARD

Dalia Topelson

As people are moving information previously hidden in locked file cabinets or safes into their personal clouds, companies have inadvertently gained unprecedented power over who can access and control information about individual citizens. This shift in control over personal data to the private corporate sector has created a new guard of corporate intermediaries that, by circumstance, have unwittingly become arbiters of law. Corporations, rather than individuals and judges, are deciding when and how information should be shared, destroyed, taken down, or concealed. The result is a disconnect between individual citizens and the judicial process that robs individuals of the opportunity to protect their rights and interests in the courts, including their right to free expression and to be free from unwarranted searches and seizures. In light of the revelations regarding the National Security Agency's large scale collection of data from consumer technology service providers, it is imperative that we analyze the role companies play in managing data collected and stored on behalf of individual citizens, including the legal structures that regulate (or don't regulate) what companies can and cannot do with an individual's information. The need is even more urgent in light of the growing investment in "big data" by venture capitalists and the like.

At present, companies in the United States are incentivized both economically and legally to take a passive approach when confronted with a takedown request or a government request for information. Challenging a request creates legal costs and puts companies at risk of direct liability for failing to comply with the request or to exercise their right to safe harbor protections offered by the law. In order to challenge a request, a company must assess its legality, but most companies lack the expertise and authority to make these types of judgment calls. This structure is further reinforced in companies' terms of use and privacy policies, which often give companies sweeping rights to disclose information as they deem necessary. The result is that governments and individuals alike can take advantage of companies' rational apathy and ignorance to obtain or suppress information uploaded by individuals to these services. This rational, yet passive, corporate behavior comes at cost to individuals, who are progressively using online tools for political expression, creating activist networks and generally championing democratic values.

Large online service providers are starting to address this problem head on by challenging these types of requests in the courts. Twitter has gained a reputation for protecting its users against unwarranted government requests,[1] and Yahoo has recently gained some praise for quietly challenging the legality of a government order requesting information under the Protect America Act.[2] Other service providers are offering encrypted email, texting, phone, and video chat services to help individuals proactively protect online communications from being intercepted. Still, most companies lack the legal resources and expertise to challenge these types of requests, and as a society, we should ask ourselves whether we want to relinquish control over the judicial process to intermediaries whose interests may be at odds with our own. This is not to say that companies should stop implementing policies and processes to help protect their customers from unwarranted intrusions of privacy or suppression of protected speech. Rather, we should revisit existing legal mechanisms and structures to ensure that we as citizens are capable of exercising our right to due process to protect the civil rights and liberties that create the foundation for a free democratic society.

Notes

1. Kim Zetter, "Twitter Fights Back to Protect 'Occupy Wall Street' Protester," Wired, August 27, 2012, http://www.wired.com/threatlevel/2012/08/twitter-appeals-occupy-order/. See also Rachel Weiner, "Twitter earns plaudits for privacy amid NSA controversy," The Washington Post, June 7, 2013, http://www.washingtonpost.com/blogs/post-politics/wp/2013/06/07/twitter-earns-plaudits-for-privacy-amid-nsa-controversy/.
2. Mark Rumold, "Yahoo's Fight for its Users in Secret Court Earns the Company Special Recognition in Who Has Your Back Survey," Electronic Frontier Foundation, July 15, 2013, https://www.eff.org/deeplinks/2013/07/yahoo-fight-for-users-earns-company-special-recognition.

THE COMMERCIALIZATION OF CENSORSHIP AND SURVEILLANCE

Ron Deibert and Masashi Crete-Nishihata

The commercial market for Internet filtering and surveillance technologies is rapidly growing. This market consists of a range of products capable of content filtering and both passive and targeted surveillance, which, depending on the end use, can serve legitimate purposes or result in human rights violations. For example, products used for managing network traffic and restricting access to web content in private enterprise and institutional settings can also be used by governments to censor content on the national level or engage in passive surveillance.[1] Other technologies such as "lawful intercept" products are designed to provide passive and targeted surveillance capabilities, and are typically marketed directly to government agencies.

There are numerous examples of such technologies in the current marketplace. The US-based company Blue Coat provides network management appliances including PacketShaper and ProxySG, which are capable of network filtering and surveillance.[2] The Canada-based company Netsweeper develops products specifically designed to filter web content. The UK-based company Gamma International sells FinFisher, "governmental IT intrusion" software that can exfiltrate data, intercept email and instant messaging communications, and spy on users through webcams and microphones.[3]

These technologies have come under increased scrutiny over their use by regimes with dubious human rights records. Following the 2011 the Egyptian revolution, protestors retrieved a document from state security offices outlining an offer to the Egyptian State Security Investigations Service for the Finfisher surveillance software package. Similarly, in 2011 the *Wall Street Journal* reported that the French company Amesys sold deep packet inspection systems to the Gaddafi regime, and that the Gaddafi regime purchased technology from China's ZTE and South Africa's VASTech capable of tapping international phone calls. Bloomberg reported that Sweden's Ericsson, the United Kingdom's Creativity Software, and Ireland's AdaptiveMobile all provided Iranian law enforcement and state security agencies with surveillance technology. Privacy International believes that at least thirty British companies and at least fifty US companies sold surveillance technologies to countries that have committed human rights violations. [4]

From the mid-2000s onwards, the Citizen Lab has documented numerous cases of products developed in North America and Europe being used for censorship and surveillance by governments with poor human rights records, and in some cases under international sanctions.[5]

In more recent work, the Citizen Lab has revealed evidence of Netsweeper's filtering products in Pakistan, Qatar, the UAE, and Yemen.[6] The Citizen Lab has also found Blue Coat devices on public networks in 83 countries, including those with questionable human rights records, such as Burma, Cote d'Ivoire, and United Arab Emirates; and countries subject to sanctions, including Iran, Syria, and Sudan.[7] These findings raise questions around the sale of "dual-use" information and communication technologies to national jurisdictions where the implementation of such technology has not been publicly debated or shaped by the rule of law. These issues go beyond any one company and underscore the imperatives of addressing the global public policy implications of internationally marketed communications infrastructure and services.

Products used by law enforcement and government agencies for "lawful interception" become problematic in countries with weak rule of law and where dissident activities can be viewed as criminal. In 2012, the Citizen Lab found evidence of FinFisher being used to target Bahraini activists. Since that initial finding, we further revealed evidence of FinFisher campaigns with political content relevant to Ethiopia and Malaysia. In our most recent research, we detected FinFisher command and control servers (C2s) in 36 countries. The presence of a Finfisher C2 in a country does not necessarily imply that law enforcement or government agencies of that country are clients and operators of FinFisher. However, the global proliferation of Finfisher raises questions regarding how the product is being used, particularly in countries with problematic human rights records.

Lawmakers at national and regional levels and civil society organizations have called for greater regulation of sensitive technologies through industry self-regulation or legislative measures, such as export controls and sanctions. In December 2012, the European Union passed a resolution on a "Digital Freedom Strategy" that *inter alia* called for "a ban on exports of repressive technologies and services to authoritarian regimes" and "the establishment of a list, to be regularly updated, of countries which are violating freedom of expression in the context of human rights and to which the export of the above 'single-use' items [technologies that inherently threaten human rights, such as jamming, surveillance, monitoring and interception technology] should be banned."[8]

Civil society groups, policymakers, and others have pressured the private sector to better control the end uses of their products, leading to new frameworks for corporate social responsibility. To this end, civil society has developed a number of frameworks to encourage corporate social responsibility. For example, the Electronic Frontier Foundation's "Know Your Customer" framework encourages companies to investigate customers before and during transactions.[9]

Multi-stakeholder efforts have also emerged, such as the Global Network Initiative, a group of companies, civil society organizations, academics, and investors that provides a framework based on commitments to freedom of expression and privacy principles.[10] Some companies have developed their own corporate social responsibility policies. For example, Websense has a policy of not selling to "governments or Internet service providers that are engaged in any sort of government-imposed censorship."[11]

Ongoing research and monitoring of these technologies for censorship and surveillance is vital for informing policymakers and vendors who many not be aware that their products are being used to violate human rights. In 2009, after the OpenNet Initiative informed Websense that its products were being used to filter political content in Yemen (and thus violating the company's anti-censorship policy), Websense withdrew software update support. In 2011, the company joined the Global Network Initiative.[12] Similarly, media attention and pressure from government and civil society organizations in the wake of findings by Citizen Lab and others that Blue Coat devices were active in Syria[13] prompted the company to withdraw support, updates, and other services to active Blue Coat devices in the country.[14]

Addressing this growing market and the potential of human rights violations stemming from the use of Internet filtering and surveillance products requires dialogue between the private sector, government, and civil society. Bringing together perspectives from these stakeholders is crucial for moving towards effective options for intelligently controlling these technologies and ensuring companies can fulfill their

moral and ethical obligations while also protecting them from liabilities that could arise from knowledge gaps and / or partner malfeasance in their global operations.

Notes

1. For research on Internet filtering products being used in institutional settings, see: Peacefire: Open Access for the Net Generation, http://peacefire.org/info/about-peacefire.shtml; "Seth Finkelstein's Anticensorware Investigations - Censorware Exposed," http://sethf.com/anticensorware/; and Benjamin Edelman, "Expert Report of Benjamin Edelman," Multnomah County Public Library et al., vs. United States of America, et al., http://cyber.law.harvard.edu/archived_content/people/edelman/pubs/aclu-101501.pdf.
2. "Blue Coat PacketShaper Application List," Blue Coat, http://www.bluecoat.com/sites/default/files/documents/files/PacketShaper_Application_List.c.pdf.
3. Gamma International, "Remote Monitoring & Infection Solutions," FinFisher IT Intrusion, http://wikileaks.org/spyfiles/files/0/289_GAMMA-201110-FinSpy.pdf.
4. See Gamma International, "Remote Monitoring & Infection Solutions," FinFisher IT Intrusion, http://wikileaks.org/spyfiles/files/0/289_GAMMA-201110-FinSpy.pdf; Margaret Coker and Paul Sonne, "Firms Aided Libyan Spies," *Wall Street Journal*, August 30, 2011, http://online.wsj.com/article/SB10001424053111904199404576538721260166388.html; Ben Elgin, Vernon Silver, and Alan Katz, "Iranian Police Seizing Dissidents Get Aid Of Western Companies," *Bloomberg*, October 30, 2011, http://www.bloomberg.com/news/2011-10-31/iranian-police-seizing-dissidents-get-aid-of-western-companies.html; and Jamie Doward and Rebecca Lewis, "UK 'Exporting Surveillance Technology to Repressive Nations'," *The Guardian*, April 7, 2012, http://www.theguardian.com/world/2012/apr/07/surveillance-technology-repressive-regimes.
5. See: "Tunisia," OpenNet Initiative, 2005, http://opennet.net/studies/tunisia; "Saudi Arabia," OpenNet Initiative, 2009, http://opennet.net/research/profiles/saudi-arabia; "United Arab Emirates," OpenNet Initiative, 2009, http://opennet.net/research/profiles/united-arab-emirates; "Yemen," OpenNet Initiative, 2009, http://opennet.net/research/profiles/yemen; and Jakub Dalek, Bennett Haselton, Helmi Noman, Adam Senft, Masashi Crete-Nishihata, Phillipa Gill, and Ronald Deibert, "A Method for Identifying and Confirming the Use of URL Filtering Products for Censorship," IMC'13, October 23-25, 2013, Barcelona, Spain.
6. Helmi Noman, "When a Canadian Company Decides what Citizens in the Middle East Access Online," OpenNet Initiative, May 16, 2011, https://opennet.net/blog/2011/05/when-a-canadian-company-decides-what-citizens-middle-east-can-access-online; and Citizen Lab, "O Pakistan, We Stand on Guard for Thee: An Analysis of Canada-based Netsweeper's Role in Pakistan's Censorship Regime," June 2013, https://citizenlab.org/2013/06/o-pakistan/.
7. "Behind Blue Coat: Investigations of Commercial Filtering in Syria and Burma," Citizen Lab, November 9, 2011, https://citizenlab.org/2011/11/behind-blue-coat; Morgan Marquis-Boire et al., "Planet Blue Coat: Mapping Global Censorship and Surveillance Tools," Citizen Lab, January 15, 2013, https://citizenlab.org/2013/01/planet-blue-coat-mapping-global-censorship-and-surveillance-tools; and Morgan Marquis-Boire et al., "Some Devices Wander by Mistake: Planet Blue Coat Redux," July 9, 2013, https://citizenlab.org/2013/07/planet-blue-coat-redux/.
8. European Parliament, *Report on a Digital Freedom Strategy in EU Foreign Policy*

(2012/2094(INI)), November 15, 2012, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2012-0374+0+DOC+PDF+V0//EN&language=EN. The US State Department also issued a guide on the export of "sensitive technology" to Iran and Syria pursuant to applicable sanctions, and the British government invoked an existing international export control regime—the Wassenaar Arrangement—to assert that FinFisher was subject to export controls. See: "State Department Sanctions Information and Guidance," US Department of State, November 8, 2012, http://www.state.gov/e/eb/tfs/spi/iran/fs/200316.htm; and "British government admits it has already started controlling exports of Gamma International's FinSpy," Privacy International, September 10, 2012, https://www.privacyinternational.org/press-releases/british-government-admits-it-has-already-started-controlling-exports-of-gamma .

9. Cindy Cohn and Jillian C. York, "'Know Your Customer' Standards for Sales of Surveillance Equipment," Electronic Frontier Foundation, October 24, 2011, https://www.eff.org/deeplinks/2011/10/it's-time-know-your-customer-standards-sales-surveillance-equipment.

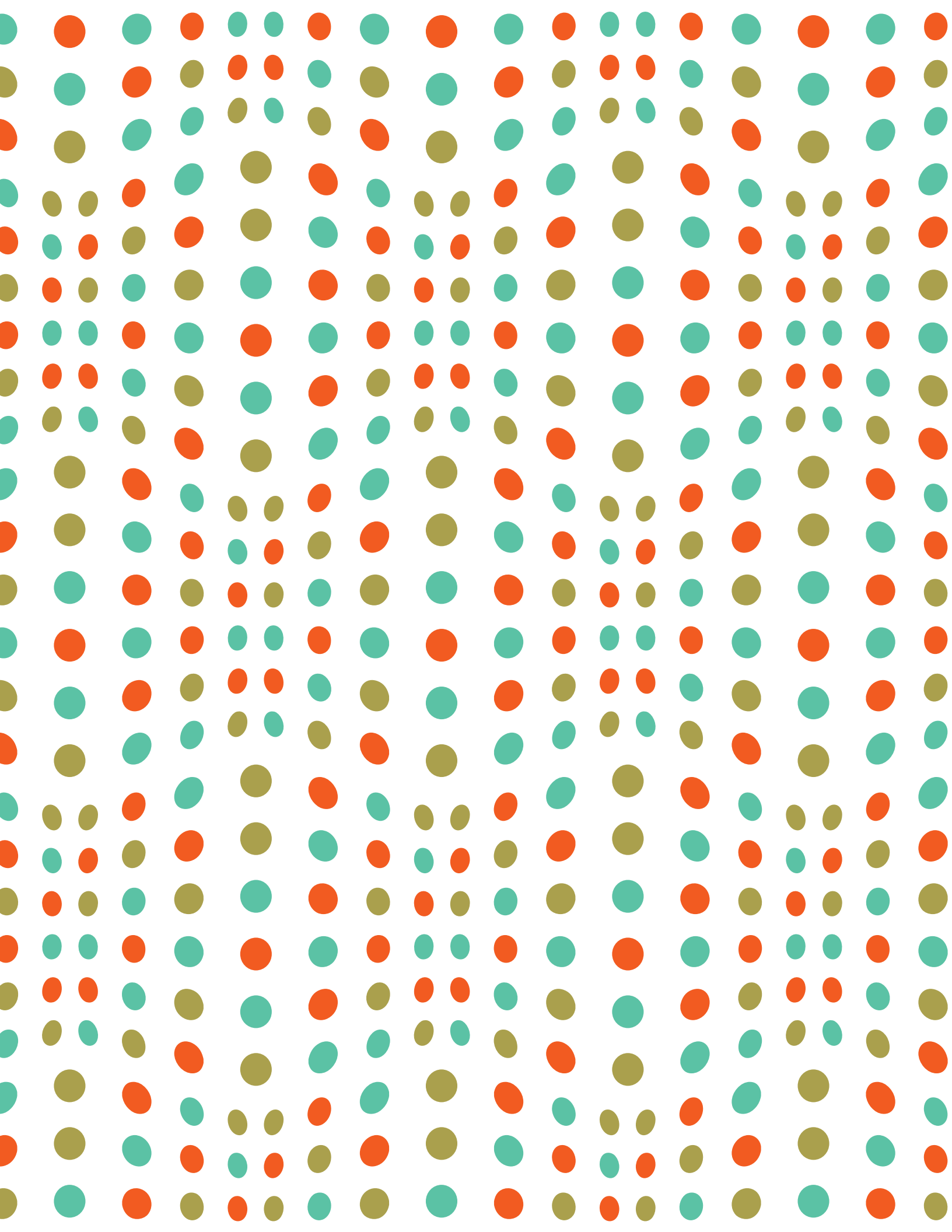
10. Global Network Initiative, http://www.globalnetworkinitiative.org.

11. "Anti-Censorship Policy," Websense, http://www.websense.com/content/censorship-policy.aspx.

12. Jillian C. York, "Websense Bars Yemen's Government from Further Software Updates," OpenNet Initiative, 2009, https://opennet.net/blog/2009/08/websensebars-yemens-government-further-softwareupdates.

13. "Web Censorship Technologies in Syria Revealed," Reflets.info, August 12, 2011, http://reflets.info/opsyria-web-censorship-technologies-in-syria-revealed-en; "Blue Coat's Role in Syria Censorship and Nationwide Monitoring System," Reflets.info, September 1, 2011, http://reflets.info/bluecoats-role-in-syrian-censorship-and-nationwide-monitoring-system; "#OpSyria: Syrian Censorship Logs (Season 3)," Reflets.info, October 4, 2011, http://reflets.info/opsyria-syrian-censoship-log; "Behind Blue Coat: Investigations of Commercial Filtering in Syria and Burma," November 9, 2011, https://citizenlab.org/2011/11/behind-blue-coat/.

14. "Update on Blue Coat Devices in Syria," Blue Coat, December 15, 2011, http://www.bluecoat.com/company/news/update-blue-coat-devices-syria; and Citizen Lab, "UPDATE: Are Blue Coat Devices in Syria "Phoning Home?," Citizen Lab, January 14, 2013, https://citizenlab.org/2011/11/behind-blue-coat/#update.



CITIZENS AS ACTORS

Bruce Etling

The Internet has not led to radical new forms of direct democracy, as some predicted in the early days of the Web, but it is hard to look at the major protests and political changes that have swept across the globe recently and not see myriad ways in which the Internet has empowered citizens. Online tools continue to aid citizens in efforts to check government and corporate power and to highlight cases of corruption and abuse of power. The networked public sphere has continued to mature into a political force, marked by important victories such as the thwarting of the Stop Online Piracy Act (SOPA), Protect-IP Act (PIPA), and Anti-Counterfeiting Trade Agreement (ACTA). The Internet and social media have also enabled new forms of citizen dissent, the ethics of which are still under debate, including leaks of national security information by well-placed individuals in security bureaucracies and the emergence of "hacktivism" tactics as new forms of civil disobedience. In the most advanced of Western democracies, the Internet has created additional pathways for constituents to be heard by their representatives and made it easier for citizens to participate, through mechanisms such as e-voting in Switzerland. Still, the greatest changes to the citizen-government relationship appear to be those created at the grass roots by citizens, instead of those initiated from the top-down by governments.

> ***Without the Internet, the opposition to the AKP's popular but strong-handed rule may never have made it into the streets in such a spectacular fashion.***
>
> —ZEYNEP TUFEKCI
> "I was wrong about this Internet thing": Social Media and the Gezi Park Protests

The Internet and Protests

Citizens have increasingly used the Internet and social media to mobilize and coordinate protests. In the past few years alone, the world has seen a number of mass protests, including those connected to the Arab Spring in the Middle East and North Africa, those sparked by election falsification in Russia, disputes over public park space in Turkey, protests over an increase in public transportation fares in Brazil, the Indignados movement in Spain, and the global Occupy movement. A common undercurrent in many of these protests is citizen pushback against corruption, entrenched political elites, and economic inequality. These protests were not caused by the Internet, but online tools and social media platforms have played important information-sharing, coordination, mobilization, and community-building roles when economic, political, demographic, and other structural factors have aligned to create conditions conducive for protests and political change.

The most spectacular and far-reaching examples of Internet-enabled protests remain those associated with the Arab Spring, which led to the fall of entrenched dictators in Tunisia, Libya, Yemen, and Egypt. Those events also undercut many arguments put forward by skeptics that online talk is cheap, that online activism is not real activism, that the Internet is more useful for dictators, and that the region was immune to the gradual but continuing expansion of democracy. For example, research in Egypt shows that social media, in particular Facebook, provided new sources of information that the regime was not able to counter, and that social media use greatly increased the likelihood that

individuals would attend protests on the first day, when success is typically least assured and the risk of attendance the greatest. The Internet was also critical in shaping how citizens made decisions about the logistics of protests and their likelihood of success.[1] Researchers have also found evidence that social media played a central role in shaping political debates in the region, especially among the young, urban, and well-educated; that spikes in online revolutionary discussion often preceded major offline protest events; and that social media helped spread democratic ideas across international borders.[2] However, as events in the region since 2011 have shown, while the Internet may be especially useful for protests and issue-specific campaigns, social media have yet to provide an equivalent level of support to citizens in building democracy and creating new political institutions.

A significant benefit of the Internet is that it massively reduces the costs of mobilization and coordination of collective action. Event pages on social networking sites such as Facebook, Twitter, and similar local variants provide protest leaders with easy and low-cost ways to spread the word about protests and mobilize core constituencies and for protest participants to signal their intention to participate. Protesters can then also use social media sites, including video and photo sharing sites, to show the wider public their power in numbers, share popular signs and humorous memes, develop a group identity, and expose the reaction of the state, including government-sanctioned violence.

These tools are also used to provide alternative framings of the protest movement and protest activities. For example, while many have questioned the political impact of the Occupy movement, it is clear that the movement was able to push the frame of the "99%" into mainstream public discourse. The ability to put alternative framings and agendas into the public sphere is especially important in countries such as Russia, China, and Iran, where there is strong influence over or complete control of mainstream media outlets, including both print and broadcast. These tools also offer new ways for protesters to participate in movements and contribute to campaigns through, for example, creating, posting, and remixing user-generated video. More generally, online tools have also made easier identifying affinity groups and connecting divergent groups and parts of society that might have vastly different political platforms, but come together at times of political discontent and mass protests. Examples include nationalists and liberals in Russia united behind a common protest banner and Islamists, leftists, and youth movements in Egypt in the anti-Mubarak protests in 2011. Finally, the Internet and social media have created a public space for experimentation and learning at a local, national, and international level. This enables the diffusion of protest ideas and also allows movement leaders in one place to see what is working and what is not, and then adjust strategy, tactics, framings, and organizational efforts for greater success given local conditions.

In many cases, offline protest events are still critical for these movements and issue campaigns; the success of exclusively online action is still quite rare. However, in defeating the SOPA/PIPA legislation, online actions were probably much more important than the small, offline protests held in cities across the United States. The mix of offline and online organization also varies depending on the individual movement. For example, in Brazil's recent protests, offline organizational efforts by the Free Fare movement seem to have been important to organization of the initial protests, and helped to lay a foundation of dissent before just a small increase in transportation fares ignited large-scale protests. Those protests grew larger than anything seen before by organizers thanks at least in part to social media, and video evidence of police brutality also helped pull more Brazilians to the side of the protesters. It is worth highlighting that the Internet has been especially helpful for protests and

issue-specific campaigns, but in many instances has not led online protest leaders to run for office, create political parties, or otherwise participate in mainstream politics (although there have been exceptions, including in Russia, Tunisia, and the Tea Party in the United States).

While the media and many scholars tend to emphasize more positive examples of social media empowering democratic social movements and civil society, the Internet does not pick favorites. Those that society has intentionally marginalized from the political process—including extremists, nationalists. and nativists—can just as easily use the Internet. Still, those with ideas that are on the margins and have little support to begin with rarely gain mass followings solely because of a larger potential audience on the Internet. It may be easier for such individuals to find each other than it was in the past, but this does not mean their ideas have become more popular.

An Accountability and Fact-Checking Platform

Citizens living in a range of international settings and under various regime types continue to use the Internet as a check on corruption, mismanagement, and abuse of power by governments, corporations, and political and economic elites. China has provided a number of examples where netizens have been able to highlight corruption and malfeasance, abuse by local officials, and cover-ups of scandals that the government-controlled media would not cover. Examples include the tainted powdered milk formula scandal in 2008, the infamous Wenzhou high-speed train crash, and numerous examples of land disputes and ecological disasters. As a check on corporations, we also see cases where workers are increasingly expressing their demands for better pay and working conditions to international customers and national leaders, such as multiple strikes by employees of technology producer Foxconn.

> ***This past year has shown an especially significant rise in the prominence of primary source material originating from members of the general public. In numerous significant instances, individuals have engaged with primary source material to supplement mediated news content or highlight under-reported issues.***
>
> —JEFF HERMES AND ANDY SELLARS
> The Role of Citizens in Gathering, Publishing, and Consuming Primary Source News Content

Online communities are able to bring issues to the forefront of the public debate that would not occur otherwise, especially where political or economic elites have control over national media. Citizen journalism platforms, including Canada-based NowPublic, Global Voices internationally, and Ridus in Russia, among others, play an important role in surfacing and publicizing cases of corruption and abuse of local leaders. At least in China, the central government seems willing to let local leaders take the fall when this type of corruption and abuse become publicized, perhaps to let off steam in an otherwise tightly controlled political space, even if structural changes at the national level still seem far off.

The Networked Public Sphere and Issue-Specific Campaigns

The rise of social networking and digital communication technologies has facilitated the creation of the networked public sphere, broadly defined as an online public space where citizens can come together to debate and decide what issues are most salient as well as determine how to act on them. While critics argue that online organization and protests are not equivalent to those undertaken by previous generations of social movements, the networked public sphere has had some important recent victories that undermine this skepticism. The starkest examples are online efforts that killed Internet-related legislation that was pushed by the music and recording industries. In the United States, online efforts averted passage of the Stop Online Piracy Act (SOPA) and the Protect IP Act (PIPA). Soon after, the international trade agreement ACTA lost support in the face of similar civil society opposition. Individuals can play outsized roles in the networked public sphere: one example is the Houston blogger who started an online campaign to ban the use of 'pink slime' (which food writer Michael Pollan describes as a kind of industrial-strength hamburger filler made from a mix of slaughterhouse scraps and treated with ammonia) in the hamburger served in the federal school lunch program. Within days of the online petition, the USDA allowed schools to drop the product, and major supermarkets stopped carrying it. Recently though, it still seems that collectives—informal and formal civil society groups and social movements—have more effectively leveraged the Internet in support of issue-specific campaigns.

> ***Users of a number of online platforms, such as Reddit and various online gaming communities, successfully pushed technology companies to reverse their support for SOPA and PIPA.***
>
> —BRUCE ETLING
> The Defeat of SOPA, PIPA, and ACTA: The Networked Public Sphere Comes of Age

New Forms of Civil Disobedience

Networked technologies have also enabled new forms of civil disobedience. Two forms of digital disobedience have been on the rise recently: DDoS attacks that take down websites (and other "hactivist" tactics such as defacing opponents' websites) and leaks of national security information. The ethics and legitimacy of these tactics, to say nothing of the outcomes, continue to be fiercely debated. Even if consensus never emerges, it seems very likely that these news forms of civil disobedience will continue for the foreseeable future and that they will continue to be highly disruptive to traditional legal and political institutions. Leaks certainly occurred before the Internet, but the leak by Bradley (now

> ***As familiar and widely accepted activist tools—petitions, fundraisers, mass letter-writing, call-in campaigns and others—find equivalent practices in the online space, what about tactics like street marches, picket lines, sit-ins, and occupations? Where is the space online for civil disobedience?***
>
> —MOLLY SAUTER
> The Future of Civil Disobedience

Chelsea) Manning of US diplomatic cables was unmatched in its scale and by Manning's choice to distribute the cables through the Internet via the Wikileaks website, instead of primarily through a traditional print publication.

> ***Website defacement activities during the Arab Spring have emerged as a common form of disruptive protest by rival groups.***
>
> —HELMI NOMAN
> Antagonism Uploaded: Website Defacements During the Arab Spring

The use of DDoS attacks by activists is controversial within digital activist communities. Some argue that DDoS attacks are also legitimate forms of civil disobedience. Others view such activity as akin to digital vandalism. These types of attacks have taken place for decades, in support of a range of different causes, from the Zapatista movement in Mexico to more recent DDoS attacks both in support of and against Wikileaks. DDoS attacks are also frequently used by proxies of the Russian, Chinese, and Syrian governments to attack domestic and international opponents of those regimes. In the case of the Russian election protests, DDoS attacks were also used by the Russian branch of Anonymous to take the website of the pro-Putin youth group Nashi offline. Hackers also released internal Nashi emails that purportedly proved that the group pays journalists and online communities for positive coverage of itself and the Russian government.

The long-term political impacts of these new forms of civil disobedience remain unclear. The Manning case does not seem to have led to any major changes in US foreign policy or to drastic shifts in US public opinion against the wars in Iraq and Afghanistan, and Manning has since been sentenced to 35 years in prison. The US State Department cables Manning leaked to Wikileaks appear to have had a larger impact in other countries. For example, the leaked cables appear to have played a role to the Arab spring protests after they were used by activists to attest to the corruption and excesses of the rulers at the time. The evolving Snowden case, however, has led to a national and global conversation about US government surveillance practices, the role of private companies in these practices, and user privacy. The efficacy of DDoS attacks is not entirely clear either, since most sites come back online fairly quickly. DDoS and other hacker attacks seem most useful in raising awareness and gaining attention for social movements, a critical issue for all activists who, even in the new media ecosystem, still struggle to gain attention among the many new voices and sources of information available in the broader media ecology.

> ***The technical underpinnings of our digital interactions are so complex that the average Internet user doesn't have the know-how to build their own tools to browse the web, much less to interact securely and privately online. Instead, consumers rely on "free" platforms built by software companies to communicate and browse the Internet.***
>
> —ASHKAN SOLTANI
> The Privacy Puzzle: Little or No Choice

Despite the success of citizens in pushing back against governments and corporations, large institutions continue to dominate the Internet space. This makes it difficult for individuals to act autonomously and securely

online, especially for activists who may work at cross-purposes to both corporate and government interests. Platforms and software exist that can help citizens counter this trend, such as anonymizers and tools for encryption and secure email and speech. Unfortunately, these tools have not yet gained wide adoption beyond the most tech-savvy of users, but that may change as a result of revelations about the reach of NSA and other government surveillance programs. The renewed interest in these tools was demonstrated recently by the tremendous increase in subscribers to Lavabit's secure email service, whose owner ultimately closed the company instead of betraying his promise to provide secure email to his customers. But this example also points to a weakness of these tools, as they are often run by small companies or groups of users that do not have the legal and lobbying clout to push back against governments.

> ***On June 30, 2013 prompted by revelations of surveillance programs in the US and UK, former Union of International Associations Assistant Secretary-General Anthony Judge published a detailed proposal titled "Circumventing Invasive Internet Surveillance with Carrier Pigeons."***
>
> —REX TROUMBLEY
> Flying Past Firewalls: Pigeons as Circumvention Tools?

Conclusion

Digitally mediated collective action by individuals and groups is constantly evolving as activists continue to experiment, learn, and adapt from one another and from the reaction of states, corporations, and other power holders to their efforts. Recognizing the importance of online, grassroots support, corporate and state actors are increasingly trying to harness the power of the Web as well. It is unclear if governments and corporations will be able to create "astroturf" online communities that have the authenticity and legitimacy of emergent protest movements, but it may be enough to sow fear, uncertainty, and doubt through well-financed misinformation campaigns. It is also unclear how widely the lessons of single-issue campaigns such as SOPA/PIPA can be applied, or if new forms of digital disobedience will ever be accepted by majorities as legitimate political acts. The power dynamic between governments, corporations, and citizens has not been totally overturned, but digitally empowered civil society actors continue to disrupt that status quo in ways that was hard to imagine even just a few years ago, and on a global scale that has surprised even the most optimistic among us.

Notes

1. Zeynep Tufekci and Christopher Wilson, "Social Media and the Decision to Participate in Political Protest: Observations From Tahrir Square," Journal of Communication, 62 (2012) 363-379.
2. Philip N. Howard, Aiden Duffy, Deen Freelon, Muzammil Hussain, Will Mari and Marwa Mazaid, "Opening Closed Regimes: What was the Role of Social Media During the Arab Spring?", Project on Information Technology & Political Islam: http://pitpi.org/wp-content/uploads/2013/02/2011_Howard-Duffy-Freelon-Hussain-Mari-Mazaid_pITPI.pdf.

"I WAS WRONG ABOUT THIS INTERNET THING": SOCIAL MEDIA AND THE GEZI PARK PROTESTS

Zeynep Tufekci

"I was wrong about this Internet thing."

I heard this sentiment again and again during my interviews at Gezi Park, Istanbul, during the height of the protests in June 2013. The protests were sparked by top-down plans to raze a small park in the city's historic Taksim square in the Beyoğlu district, an area known for its concentration of artists, nightlife, and theaters, and to replace it with a shopping mall and a hotel fashioned as a replica of the Ottoman Barracks that had once stood where the park was.

This growing realization of the Internet's power came from middle-aged people who had previously chided youth for their attachment to screens, phones, and social media. Yet when Turkey's heavily self-censored corporate media—owned by large conglomerates that vie for lucrative construction, energy, and urban renewal contracts from the government and that use their mass media outlets as a means to curry favor with the powerful ruling party, the AKP—broadcast penguin documentaries and cooking shows while ignoring the multi-day clashes between protesters and the police at the center of the most populous city in the country, it was social media that got the news out to the bewildered, angry residents of Istanbul.

At least 50 percent of the population of Turkey is online, most through broadband connectivity. Mobile devices are ubiquitous as well—the number of cell phone subscriptions cover about 90 percent of the population. Twitter has become the medium of choice for the protesters, who favor it for its lightweight applications on mobile devices, short texts, and ability to get news with pictures out quickly to large numbers of people. With estimates as high as 39 percent of Turkey's Internet users adopting the platform, and daily "trending topics" wars between supporters of AKP and Gezi protesters, it was not a huge surprise when the Prime Minister Erdogan singled out the platform and called it a "menace to society. The biggest lies are all there."[1]

Many protesters were convinced that without Twitter's ability to spread news quickly and widely, they could not have organized such large-scale action. Many had wrestled with the problem of false reports on Twitter, targeted by Erdogan as an indication of platform's untrustworthiness, and had undergone a crash course on social media literacy. "I have learned which accounts to trust and how to verify information," many told me. Others went a step further: "If I hear of clashes, I personally try to get there and take a picture to provide proof," a protester told me, while showing a wound in his leg from being hit with a tear gas canister while on a mission to verify and report.

Despite AKP officials' blatant dislike of social media as source of dissent, the Internet was not unplugged either in the Gezi Park or in the country, nor were any of the platforms shut down. Instead, the AKP seems to have decided on a strategy of engaging in a public relations blitz on social media by hiring "6,000 social media experts" itself,[2] increasing its efforts to force social media companies to open offices in Turkey so that the government can acquire user IP's in response to court rulings (currently Facebook and Google have offices in Turkey, but Twitter does not), and relying on its total dominance of mass media. In fact, polls showed that majority of AKP supporters believed that the

protests were "organized by foreign sources," a claim repeated multiple times by the prime minister and other AKP officials on mass media. AKP officials have also announced that they will pass new laws to "regulate misinformation" on social media—sending a clear signal that Turkey's Internet users will come under close scrutiny.

However, Turkey's electoral system, designed by generals in the 1980 coup, makes it very hard for new parties to break into the parliamentary system. This barrier, coupled with the incompetence of legacy opposition parties—which cannot be replaced, thanks to the said electoral system—and the AKP's own powerful electoral machinery, makes it unlikely that a social media-organized opposition will mount an effective electoral challenge in the 2014 elections.

Without the Internet, the opposition to the AKP's popular but strong-handed rule may never have made it into the streets in such a spectacular fashion. It remains to be seen if they can find their way into the voting booth in the face of corrupt mass media, a skewed electoral system, and a smart, powerful, and dominant ruling party that is ready to both beat them and join them online.

Notes

1. Will Oremus, "Turkish Prime Minister Blames Twitter for Unrest, Calls It 'the Worst Menace to Society,'" Slate, June 3, 2013, http://www.slate.com/blogs/future_tense/2013/06/03/turkey_protests_prime_minister_erdogan_blames_twitter_calls_social_media.html.
2. Ayla Albayrak and Joe Parkinson, "Turkey's Government Forms 6,000-Member Social Media Team," Wall Street Journal, September 16, 2013, http://online.wsj.com/article/SB10001424127887323527004579079151479634742.html.

THE ROLE OF CITIZENS IN GATHERING, PUBLISHING, AND CONSUMING PRIMARY SOURCE NEWS CONTENT

Jeff Hermes and Andy Sellars

For over a decade, scholars have noted the increased role that those outside the institutional press play in informing the public. This past year, however, has shown an especially significant rise in the prominence of primary source material originating from members of the general public. In numerous significant instances, individuals have engaged with primary source material to supplement mediated news content or highlight under-reported issues. This engagement has involved both the gathering of primary source material to share with others and the collective analysis of such material by loosely-connected networks of experts, analysts, and commentators.

Over the past year, several major news stories were broken by concerned citizens and activists gathering and disclosing direct evidence of government and political activity, including the videos shot by citizens of Damascus documenting the use of chemical weapons in the Syrian civil war; the "47 percent video" recorded by a member of the catering staff at an event held for presidential candidate Mitt Romney; the PRISM slide deck and other NSA materials disclosed by Edward Snowden to The Guardian; and the "lady in red" photo of Ceyda Sungur, which served as a unifying moment for anti-government protests in Turkey. This year has also brought unexpected collaboration between citizen media and law enforcement, including during the investigation into the Boston Marathon bombing, where the FBI actively solicited terabytes of eyewitness photographs and video to help identify the bombers.

In the United States, courts have begun to recognize a constitutional right of citizens to engage in this form of direct documentation, at least when directed at the actions of the government. Following the 2011 decision of a federal appeals court in Glik v. Cunniffe, a second federal appellate court recognized a First Amendment right for citizens to record the police in ACLU v. Alvarez. Marking a rare intervention in the behavior of state law enforcement, the Department of Justice's Civil Rights Division also stepped in to support the rights of citizens to record the police in a case pending in federal court in Maryland, Sharp v. Baltimore Police Department.

Private organizations, including MuckRock, Open Corporates, OpenGov, and MapLight, continue to provide resources to facilitate access to public records and government data and publish relevant documents. Judicial attention to transparency with electronic government records has increased concurrently, punctuated in the United States by cases addressing GIS mapping data and access to government document metadata. Meanwhile, a number of organizations, including Public.Resource.Org, SCOTUSblog, and the Oyez Project, have obtained funding, favorable judicial rulings, or other support for efforts to mirror general government data on their own websites.

While the creation and surfacing of primary source material by citizens has been seriously questioned only when the source breaches a duty of confidentiality over the information disclosed, such as the disclosures of Edward Snowden, significantly more criticism has been voiced as citizens move from documentation roles into analysis roles. This complexity was best highlighted during the events surrounding the Boston Marathon bombing. While public documentation of the incident was critical to the law enforcement investigation, the public's desire for information at a rate faster than the

government (or traditional news sources) would provide it led many citizens to try to parse primary source material directly. The results of these efforts were mostly negative; attempts to locate the bombers using online platforms like Reddit (on early iterations of /r/findbostonbombers) and to gather more information on the day of the Tsarnaev manhunt by listening to police scanners led to misidentifications and confusion – although similar criticisms were appropriately leveled against institutional news outlets for similar behavior. The increasing social recognition of traditional media ethics around verification of information posted on these sites has led to a richer and more expedient dissemination of information than traditionally thought possible through institutional media outlets.

The increased role of citizens in surfacing and analyzing documents has helped break news stories and improve public understanding of issues, but not all government activity with respect to primary source material has favored publication. Even in the United States, a nation that prides itself in transparency and free speech, the government has aggressively punished some of these disclosures. This has included a notorious criminal prosecution against activist Aaron Swartz for gathering thousands of academic articles for an undisclosed future use, which received significant attention and scrutiny following Swartz's suicide. The Department of Justice also obtained a conviction against Andrew Aurenheimer for accessing an unprotected AT&T website, escalating the charges from a misdemeanor to a felony based on Aurenheimer's disclosure of the data he obtained from the AT&T website to news website Gawker as evidence of AT&T's security vulnerability. (This case is now on appeal.) In August 2013, the United States also sentenced Chelsea Manning to 35 years in military prison, following her disclosure of thousands of documents to the organization Wikileaks. The position reflected in the pending federal shield bill—that citizen media and organizations dedicated to surfacing primary source material are not "journalists" worthy of protection—further underscores the continuing reluctance of the government to recognize the critical role that primary source material plays in informing the public.

THE DEFEAT OF SOPA, PIPA, AND ACTA: THE NETWORKED PUBLIC SPHERE COMES OF AGE

Bruce Etling

Arguably the most striking example of the rise of the networked public sphere as a political force is the reversal of support for the Stop Online Privacy Act (SOPA) and the Protect IP Act (PIPA) in the United States, and the international trade agreement ACTA, which lost support after the successful defeat of SOPA and PIPA.[1]

A number of successful tactics were used to support the movement, which culminated in January 2012 when millions of citizens contacted Congress to voice opposition to the legislation. Specialized tech media news outlets such as Tech Dirt, which exist primarily as web native media, as well as groups dedicated to digital freedoms, including Public Knowledge, the Center for Democracy and Technology, and the Electronic Frontier Foundation, played a critical role in sounding the alarm early and pushing the issue into the mainstream public sphere. Major online platforms and their communities of users, in particular Wikipedia, blacked out their websites and simultaneously pointed US voters to contact information for their elected representatives in Congress. Critically, the technology industry was also opposed to the legislation, although opposition was not universal. Google in particular, with its huge online user base and lobbying power, was also a major player in coming out against the legislation, placing a banner on its site in opposition to the legislation and connecting users to their Congressional representatives.

Users of a number of online platforms, such as Reddit and various online gaming communities, successfully pushed technology companies to reverse their support for SOPA and PIPA. A superb example is the Reddit community's boycott of web-hosting company Go Daddy, where a single user mobilized the community to begin moving their websites to other domains. The boycott quickly led Go Daddy to withdraw its support for the legislation. The online community was also able to draw on and promote expert commentary and analysis by Internet engineering pioneers to rebut the claims made by the content industry. Bloggers also used the space to take down the specific claim that the cost of piracy in the US is $58 billion, a number bloggers showed was vastly overblown and based on faulty assumptions.

These tactics may not be applicable against all types of legislation; they also appear to be less effective in countries with less democratic forms of government. For example, although the international agreement ACTA was stalled after the SOPA/PIPA reversal in the United States, the online community in Russia was not able to stop the passage of recent Internet legislation that now allows deep-packet inspection and gives the Russian government the ability to take down websites. This occurred even though opponents to the legislation adopted many of the same successful tactics used against SOPA/PIPA, including a blackout of Russian Wikipedia, support from Russian technology companies and their leaders, and active opposition from the Russian online community. Further, even in the United States, this type of online action cannot necessarily overcome a well-funded lobbying and advertising campaign by major industry players, as seen with the reversal of public opinion against Proposition 37, a GMO labeling initiative in California. That initiative saw opinion swing from solidly opposed (by nearly 3 to 1), to eventual passage by 3 percent at the polls thanks to a multi-million dollar adver-

tising blitz by the chemical industry (most prominently Monsanto), major processed food companies, and grocers. Money and corporate influence have not been eliminated from the political process, but there have been some important victories when the legislation concerns the Internet and in places where governments are responsive to citizen demands and public opinion. Still, it may also be the case that SOPA and PIPA are a harbinger of future online civil society action, as the tools and tactics used in this case gain adoption by civil society more broadly.

Notes

1. For a detailed analysis of this case see: Yochai Benkler, Hal Roberts, Rob Faris, Alicia Solow-Niederman, and Bruce Etling, "Social Mobilization and the Networked Public Sphere: Mapping the SOPA-PIPA Debate," July 25, 2013, http://cyber.law.harvard.edu/publications/2013/social_mobilization_and_the_networked_public_sphere.

THE FUTURE OF CIVIL DISOBEDIENCE

Molly Sauter

This article previously appeared in a different version on the Io9 website.

The Internet is a central zone for political organizing. When there is a message to get out or a group to build, most people will turn to the Internet and the tools and networks on it. Online, people sign petitions, investigate stories and rumors, amplify links and videos, donate money, and show their support for causes in a variety of ways. But as familiar and widely accepted activist tools—petitions, fundraisers, mass letter-writing, call-in campaigns and others—find equivalent practices in the online space, what about tactics like street marches, picket lines, sit-ins, and occupations? Where is the space online for civil disobedience?

The affordances of networked technologies mean our opportunities for effective political activism have increased exponentially. Where activists once put their physical bodies on the line to fight for a cause, they can now engage in digitally based acts of civil disobedience from their keyboards. Digitally based civil disobedience is developing along three major lines: Disruption, Information Distribution, and Infrastructure. Each works to empower the public, and each has its own particular challenges and benefits.

Disruptive tactics like distributed denial of service actions and website defacements have a fairly long history in Internet terms. Activists groups like the Electronic Disturbance Theater, the Strano Network, pro-Palestinian groups, and others used DDOS and website defacements in their campaigns as early as the mid-1990s. These tactics disrupt the normal flow of information, directing attention to a cause and message. Disruptive tactics are popularly focused: they aim to deliver a message to as many people as possible, by either exposing them to disruption and dissent, recruiting them to take part, or both. To be effective, this type of civil disobedience needs to attract the attention of the public, typically through the mainstream media. If the media doesn't recognize or cover the actions as acts of protest, then the activist message falls flat. (If an activist defaces a corporate website, and no one sees it, does it have political impact? Probably not.)

Information Distribution-based tactics are built around the acquisition and release of information that someone doesn't want someone else to have. In the past three years, we've seen whistleblowing, information exfiltration, doxxing (releasing personal information, such as addresses and social security numbers, about others online), and crowdsourced vigilante investigations become the tactics of choice for groups such as Wikileaks and Anonymous and those they inspire. These tactics, in one way or another, move information from a state of low visibility to one of high visibility. Crowdsourced vigilante investigations and "human flesh search"-style manhunts try to bring public attention to injustices in cases where traditional law enforcement avenues seem to have failed. Anonymous has been developing this tactic in the US and Canada with Steubenville, #JusticeforReteah, and other operations. "Human flesh search" message boards are already popular in China, giving netizens the chance to bring formerly untouchable corrupt officials to justice. The FindtheBostonBombers subreddit was a homegrown example of this kind of crowdsourced vigilante investigation. The goal of this class of tactics is to empower people to take action by adding to the information landscape. Whistleblowers and leakers rely on the cooperation of the mainstream media to publicize, contextualize, and analyze

the information they release. This may become easier as more news organization recognize open paths for whistleblowers and leakers. Wikileaks' five media partners for the Cablegate documents, the New Yorker's Strongbox program, and the Guardian's extensive work with NSA whistleblower Edward Snowden are all examples of how cooperation between whistleblowers and news organizations is growing.

Infrastructure-based activism involves the creation of alternate systems to replace those that have been compromised by state or corporate information-gathering schemes. Tor, Diaspora, and identi.ca are examples, as are the guerrilla VPNs and network connections that often spring up—generally provided by activists in other countries—to serve embattled areas. Similar to living off the grid, these projects provide people with options beyond the default. Open source or FLOSS software and Creative Commons follow the same generative ideology: when the system stops working, create a new system. The challenge is to bring these new systems into widespread use without allowing them to be compromised, either in terms of ideology or of security for users. However, these new systems often have to fight network effects as they struggle to attract users away from dominant systems: Diaspora faced this issue with Facebook. Without being able to disrupt dominant systems, user migration is often slow and piecemeal, lacking the impact activists hope for.

Disruption, Information Distribution, and Infrastructure tactics and strategies are often practiced by separate groups working independently on different issues. Sometimes these groups' interests will overlap, as when Anonymous launched the disruptive Operation Payback in support of Wikileaks during Cablegate, but there is little inter-group organization. As the practice of civil disobedience develops online, those who favor different styles of activism but who are united in a common cause should organize themselves into affinity-based coalitions, building alliances for more effective activism. Effective digitally based civil disobedience needs a diverse, integrated repertoire of contention from which to draw. A disruptive action targeting Facebook could drive users toward alternate, more open, social networking services. A leak detailing government intelligence abuses could spur disruptive protests, consumer flight to uncompromised services, or further leaks.

As digital activism develops, civil disobedience will continue to a be vital tool for expressing dissent. The tactics and strategies of Disruption, Information Distribution, and Infrastructure provide many avenues for activists for activists to work together in concerted, effective campaigns. The Internet offers the unique opportunity to organize across geography, allowing for the creation of robust global affinity groups. To be the most effective, digital activists need to work together across the lines of tactics and strategy. The future of digital civil disobedience lies in inter-group, cross-border cooperation that combines the tactics and strategies of Disruption, Information Distribution, and Infrastructure-based activism.

ANTAGONISM UPLOADED: WEBSITE DEFACEMENTS DURING THE ARAB SPRING

Helmi Noman

The popular uprisings in the Middle East and North Africa (MENA) in 2011 polarized citizens in the region. People on both sides of the conflict took up their causes online, hacking and defacing websites, comment spamming on opponent Facebook pages, and using phishing URLs to gain access to targets' online accounts. Website defacement activities during the Arab Spring have emerged as a common form of disruptive protest by rival groups—a way not only to sabotage opponents' online presences but also to disrupt the flow of information and spread opposing messages during conflict.

Website defacements are not a new tactic in the region: these types of attacks took place earlier in the context of the Israeli-Palestinian conflict, in the antagonistic relationship between Morocco and Algeria over Western Sahara, and in the religiously motivated defacement of websites between Sunni and Shiite hacker groups. These activities were rare and limited in scope, but during the MENA uprisings, information operations conducted by politically motivated groups emerged online in a newly organized and intensive way.

One of the most widely active and visible of these groups is the Syrian Electronic Army (SEA). The SEA was organized in May 2011 and tends to target groups and individuals that the Syrian regime has singled out for supporting regime change.[1] The SEA has defaced the websites of public figures such as political cartoonist and outspoken critic of the regime Ali Ferzat, Syrian composer Malek Jendali, and Syrian singer Asalah Nasri, all of whom have been harassed by Syrian security forces or the Syrian Ministry of Information. The SEA has also defaced independent news and opinion websites such as Transparent Sham and Hadatha for Syria. As the conflict in Syria came under closer international scrutiny in mid-2013, the SEA began to focus more on compromising the Twitter accounts and websites of high profile international media organizations, choosing targets such as the New York Times based on their perceived biased coverage of the events in Syria.

Anti-government groups took a similar course of action: in February 2012, anti-regime hackers defaced Syria's pro-regime Addounia TV website by replacing the content of the front page with a defacement message that included links to YouTube clips of the regime's forces cracking down on protesters. Earlier in the same month, the TV's mobile news service was compromised, with the perpetrators sending "news alerts" supporting the uprisings.[2]

In Yemen, a pro-revolution group called the Union of Yemeni Hackers targeted government-controlled media websites to protest their reporting on the uprising in March 2011. The group defaced the websites of two state TV channels, Yemen TV and Sheba TV, with messages criticizing their "distortion of the facts."

In Egypt, Mubarak supporters exchanged attacks with pro-revolution websites and groups. One group known as Sons of Mubarak compromised several Facebook pages, including one run by the Muslim Brotherhood's political organization, the Freedom and Justice Party. The group left a message on the compromised page that read, "Sons of Mubarak will punish the revolution supporters" and vowed to attack websites that refer to Mubarak as a "deposed president" and websites that produce content

that "distort the history of Mubarak." In July 2013, the website of Tamarod (an opposition group dedicated to forcing President Mohamed Morsi to call early elections) was defaced by supporters of the Muslim Brotherhood. The defacement contained a message linking to a live stream of pro-Morsi demonstrations in Cairo.

A number of other defacements have taken place in the region outside of the context of large-scale revolutionary movements. During the September 2013 protests in Sudan over fuel price increases, during which as many as 200 protesters were killed, a Sudanese government website was defaced. The defacement message criticized the governmental religious establishment's stance that "disobeying the state head or president" via street protests was haram (forbidden by God). The message asked, "Isn't killing protesters haram?" In the same month, the website of the Prime Minister of Jordan was defaced with a message protesting the increasing cost of living in the country. In October 2013, the website of an online campaign supporting the right of women to drive in Saudi Arabia was defaced with a message that claimed to reveal the name and address of the person behind the site. A later defacement message on the same site vowed to persecute those who support the campaign.

Hacking and defacing activities are not limited to internal targets. In 2011, Syrian-Turkish relations deteriorated after Syria accused Turkey of interfering in its internal affairs and supporting rebel activities; in response, Turkey accused the Syrian regime of killing civilian protesters. Syrian and Turkish hackers responded by defacing several government websites in both countries. The SEA has also defaced websites in Libya, Israel, and the United Kingdom, as well as websites outside of the region, in an attempt to disseminate Syrian regime's version of the conflict. These targets include the websites of Harvard University, Purdue University, and the Lineberger Comprehensive Cancer Center at the University of North Carolina, as well as celebrity fan sites such as johnny-depp.org, ben-affleck.us, and bradpittweb.com.

Pro-revolution hackers in Syria have also attacked targets both inside and outside the region, including the site of an Iraqi oil company (mociraq.com), where they replaced the front page with a message reading, "The Iraqi regime, backed by the Iranian regime, is supporting the Syrian regime in oppressing Syrian people." The hackers replaced the website's banners with pro-revolution insignia, along with a photo of a child who—according to protesters—was killed by Syrian security forces during one of the demonstrations. They have also targeted the websites of the Russian Embassies in India and Singapore in protest of Russia's veto of a UN Security Council resolution to condemn the Syrian government.

Ethics and appropriateness

Many hacker forums set their own broad ethical guidelines, which are primarily based on political and religious considerations rather than national legal frameworks. These guidelines often argue that the incumbent regimes and their laws are part of the problem, and therefore can be legitimately ignored.[3] Sometimes the discourse on what constitutes an appropriate act of hacking focuses on the "Islamicity" of the act, with hackers invoking Islamic legal code to determine which websites are permissible targets. Aside from Fatwa-backed near-consensus on the permissibility of defacing and even destroying websites perceived to be anti-Islamic,[4] hackers generally interpret for themselves

which targets are acceptable. Political, religious, and sectarian divides remain the main governing references used by the hackers, with hacking justified according to political grievances. Interestingly, forums where the hacking of certain political or religious sites is tolerated have themselves become targets of sabotage by rival political hackers, leading such forums to limit participation to trusted and invited members only.[5]

Identifying those behind the attacks

The groups behind the information operations described above appear to be grassroots, civilian efforts, many of which disband quickly and or go through long periods of inactivity. Linking these operations to formal entities is challenging, as most of these groups leave few digital traces. Most groups use Facebook or hacker forums to publicize their activities, claim responsibility for attacks, and recruit followers. The SEA, which has its own website, is an exception.

The SEA's domain name and web hosting subscriber can both be traced to the Syrian Computer Society (SCS), which was founded by President Bashar al-Assad in 1989 and is currently run by his brother. This information suggests the SEA enjoys at least tacit support of the Syrian regime.[6] Investigating other information operations is more challenging, though some clues exist. For example, a YouTube video exists that shows a group of young people who claim to be the Libyan Electronic Army being lectured to by an officer of the Libyan military, who tells the group that their electronic activities come second in importance only to the military itself.[7]

Verifying attribution for attacks can also be problematic, particularly as some websites show more than one defacement message claimed by different groups at the same time. For example, the website of Egypt's Social Justice Party, defaced in August 2013, showed two claims of responsibility on two different pages: one from the Yemeni Electronic Army, and another from a Moroccan group.

Final remarks

Arab Spring fallouts are likely to fuel more defacement campaigns, the scope of which is likely to increase as related social and religious contentions increasingly manifest themselves online. At the same time, the continued growth in both the quantity and quality of Arabic hacker forums is likely to produce more computerized activism and to increase the level of sophistication and potential damage of that activism. Though signs of government complicity in the current defacement campaigns are limited, it is possible that government agencies will exploit to their advantage non-state hacker groups as a proxy to hide state information operations behind anonymous grassroots activism, and to crowdsource antagonism against state opponents.

Notes

1. Helmi Noman, "The Emergence of Open and Organized Pro-Government Cyber Attacks in the Middle East: The Case of the Syrian Electronic Army," Infowar Monitor, May 30, 2011, http://www.infowar-monitor.net/2011/05/7349/.
2. SANA (Syrian State News Agency), http://www.sana.sy/eng/21/2012/02/06/398571.htm.

3. See, for example, the ethical code on the popular hacker forum Al-Jyyosh, http://www.aljyyosh.com/vb/showthread.php?t=32358 (note: forum is password protected).

4. The author discusses this issue in his book chapter, "In the Name of God: Faith-Based Internet Censorship in Majority Muslim Countries," *Routledge Handbook of Media Law* (New York: Routledge, 2013). An earlier version is available from the OpenNet Initiative at https://opennet.net/sites/opennet.net/files/ONI_NameofGod_1_08_2011.pdf.

5. The hacker forum Al-Jyyosh limited its membership to trusted, invited users after an increase in the circulation of malware by adversaries.

6. Helmi Noman, "The Emergence of Open and Organized Pro-Government Cyber Attacks in the Middle East: The Case of the Syrian Electronic Army," Infowar Monitor, May 30, 2011, http://www.infowar-monitor.net/2011/05/7349/.

7. See http://www.youtube.com/watch?v=Rh8W_CEQqTw.

THE PRIVACY PUZZLE: LITTLE OR NO CHOICE

Ashkan Soltani

The policies and common practices guiding online advertising put Internet users in a tough spot when deciding how to protect their privacy. The technical underpinnings of our digital interactions are so complex that the average Internet user doesn't have the know-how to build their own tools to browse the web, much less to interact securely and privately online. Instead, consumers rely on "free" platforms built by software companies to communicate and browse the Internet. In exchange for free services, consumers often allow these companies to track their activities and target advertising. Meaningful regulatory structure protecting users from online tracking abuses is also lacking; in fact, we even lack a clear sense of what it would mean to take advantage of a user of a free service. Currently, users must choose between accepting the options provided by these platforms and trying to independently navigate a complicated web of privacy tools and techniques. This decision is complicated by the fact that some of the do-it-yourself privacy protection measures available to consumers might put them at risk of violating arcane laws. The current policy landscape governing online tracking is woefully out of date and sometimes protects companies at the expense of consumer choice. As a result of the inconsistencies in this environment, users face a difficult puzzle when they attempt to protect their privacy.

The business model financing technology companies determines the privacy choices users are given. In the case of most platforms (browsers, social networks, phones, etc.) the model is built on monetizing consumers' data to deliver advertisements. As such, the defaults are typically set to encourage users to share information as broadly as possible to enable better targeting and measurement. While most of these companies offer users a selection of privacy settings, these are also designed with the company's bottom line in mind. This is a predictable outcome of the powerful incentive to maximize the value of user data by running complicated data mining algorithms that rely on large datasets. A selection of privacy settings can make users feel like they are in control, but these options are limited. This, combined with our knowledge that consumers rarely adjust the default settings, means that a few companies have implicit control over a majority of individual users' privacy settings.

There is no guarantee that companies will respect a user's stated preference to not be tracked, and users often lack the tools to confirm whether or not their preferences are recognized. Additionally, the companies responsible for much of this tracking are increasingly successful at circumventing blocking tools. Even if they may not undermine their own privacy setting options, they are not particularly inclined to adhere to preferences that are expressed through other vendors' software. My research has documented numerous cases of companies repeatedly circumventing the privacy settings developed by other companies that users utilize to protect their privacy. It is important to note that this kind of circumvention can violate regulations, and the Federal Trade Commission (FTC) has successfully held companies accountable for circumventing settings. So if a user (or researcher) notices a violation of this nature, there is an opportunity to rectify the situation. However, again, this depends on users being able to observe the infraction, which is far from guaranteed.

Particularly ambitious users can try to work around the sanctioned choices, but there are pitfalls here as well. There are some tools and techniques to mask online movements that a consumer could

cobble together in order to make it more difficult to track their online behavior. However, some these could be interpreted as violating the law. In particular, the Computer Fraud and Abuse Act (CFAA) poses a problem for innovations in privacy protection. The crux of a CFAA violation hinges on whether or not an action allows a user to gain "access without authorization" or "exceed authorized access" to a computer. In some cases, commonplace behaviors like managing cookies, changing browser headers, using VPNs, and even protecting one's mobile phone from being identified could be construed as an attempt to exceed authorized access to content. For example, clearing cookies is a commonly prescribed method to protect privacy (by limiting the ability for advertisers to uniquely identify a given user); however, by periodically clearing cookies—or using a browser's private browsing mode—users can easily bypass publishers' paywalls (e.g., the ten-articles-a-month limit at the New York Times). Under an unsophisticated judge's review, this could be interpreted as exceeding authorized access and is therefore a potentially prosecutable violation of the CFAA. This means that, by attempting to protect his privacy from one company, a user might "exceed authorized access" elsewhere (clearing your cookies to prevent Google from developing a profile could violate the NYT paywall).

This combination of circumstances severely limits users' choices to limit online tracking and protect their privacy. Most users stick with the business-supporting defaults set by the company and even those who deviate are still choosing among options designed to support a business model based on monetizing tracking. The ambitious users who step outside these pre-approved choices have to invest a great deal of time investigating privacy-protecting strategies and, even when they succeed in protecting themselves, may find themselves on the wrong side of the law. All of these factors make it hard to envision a way for the average Internet user to find a reasonable and effective way to protect his privacy.

FLYING PAST FILTERS AND FIREWALLS: PIGEONS AS CIRCUMVENTION TOOLS?

Rex Troumbley

On June 30, 2013 prompted by revelations of surveillance programs in the US and UK, former Union of International Associations Assistant Secretary-General Anthony Judge published a detailed proposal titled "Circumventing Invasive Internet Surveillance with Carrier Pigeons."[1] In it Judge discusses the proven competence of carrier pigeons for delivering messages, their non-military and military messaging capacity, and Chinese experiments to create pigeon cyborgs.[2] Judge acknowledges that pigeon networks have their own vulnerability (such as disease, hawks, or being lured off course by sexy decoys), but argues that others have proven pigeons are effective at transmitting digital data.

Judge's proposal has its roots in a series of earlier Request for Comments (RFC) to the Internet Engineering Task Force, the ad hoc body charged with developing and promoting Internet standards. On April Fool's Day, 1990, David Waitzman submitted an RFC on the idea of using carrier pigeons or other birds for the transmission of electronic data.[3] Waitzman called his new communication standard "Internet Protocol over Avian Carriers" (IPoAC). Nine years later, Waitzman issued a second RFC suggesting improvements to his original protocol.[4] On April 1, 2011, Brian Carpenter and Robert Hinden issued their own RFC detailing how to use IPoAC with the latest revisions to the Internet Protocol IPv6.[5]

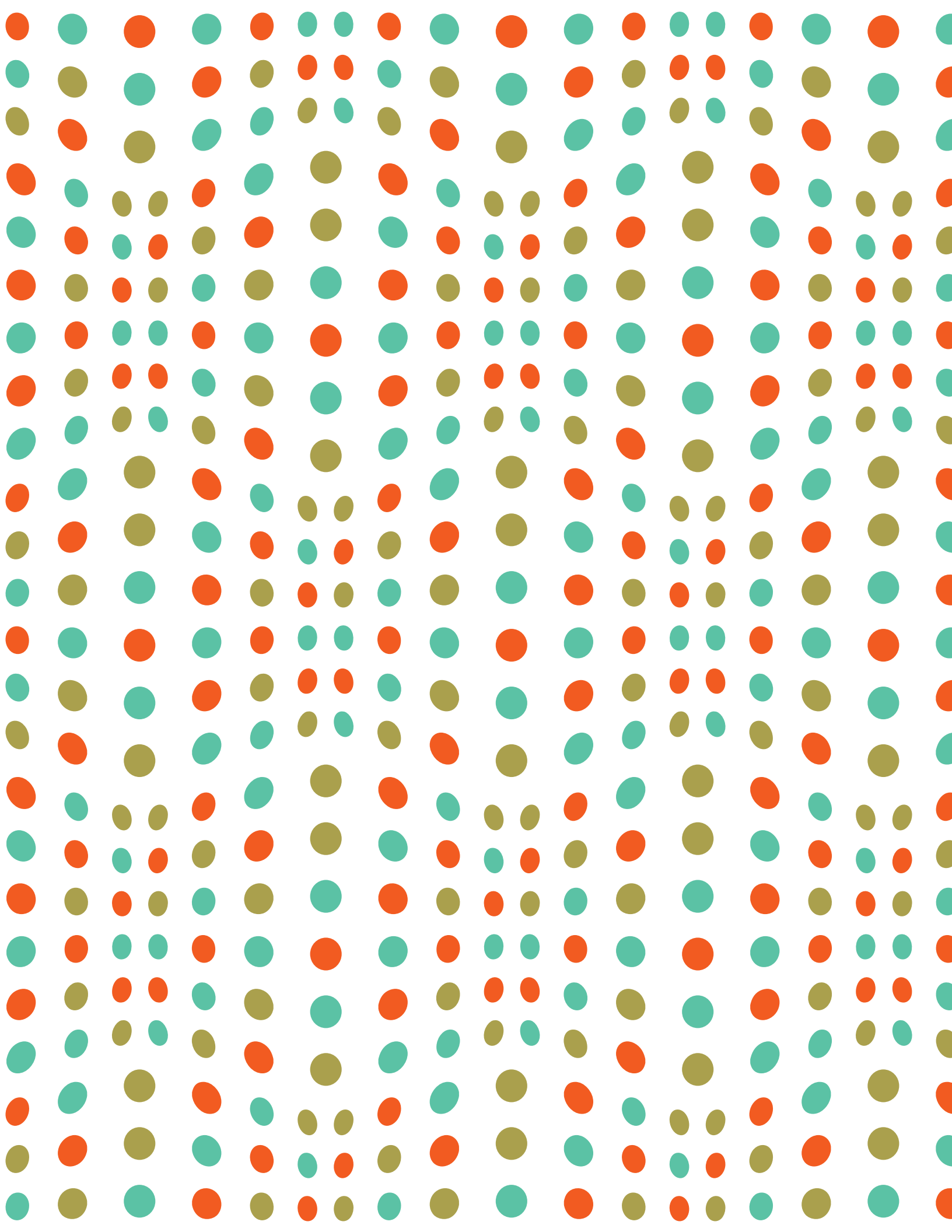
Though all three RFCs were issued as April Fools' Day jokes, in 2004, the IPoAC idea encouraged the Bergen Linux group to send nine pigeons, each carrying a single "ping," three miles. (They only received four "responses," meaning only four of the birds made it.)[6] A few years later, an IT company in South Africa raced pigeons carrying data cards against the transfer speeds of their local Internet Service Providers and easily won.[7] A similar test by an British ISP in 2010 sent a pigeon carrying a microSD card loaded with a five-minute video 75 miles in 90 minutes, beating the time it took to upload the same video to YouTube via a rural farm's Internet connection.[8]

Before the advent of the global Internet and fast data-transfer speeds, it was common to physically carry information between storage devices. "Sneakernets," or the networks of people walking around in sneakers carrying digital data, haven't gone away. After the 2011 raid of Osama Bin Laden's compound, it was discovered that Osama had been evading US intelligence organizations by using a courier to send drafts of emails stored on USB drives from a nearby Internet cafe.[9] In the Kingdom of Bhutan an offline network project distributes digital educational resources, such as Khan Academy videos and archived Wikipedia articles, to hundreds of schools with no or slow Internet access.[10] USB drives have also been used to evade Internet restrictions in North Korea and Cuba.[11]

As governments and corporations increasingly block or monitor Internet communications, and as data production continues to outpace bandwidth speed increases, sneakernets are helping move data around. Pigeon-nets may not be too far behind.

Notes

1. "Circumventing Invasive Internet Surveillance with Carrier Pigeons: Rewilding the endangered world wide web of avian migration pathways," June 30, 2013, http://www.laetusinpraesens.org/musings/pigeon.php.
2. Noah Shachtman, "Cyborg Pigeons Revealed!," *Wired*, February 27, 2007, http://www.wired.com/dangerroom/2007/02/cyborg_pigeons_/
3. David Waitzman, "A Standard for the Transmission of IP Datagrams on Avian Carriers," RFC 1149, April 1, 1990, http://www.ietf.org/rfc/rfc1149.txt.
4. David Waitzman, "IP over Avian Carriers with Quality of Service," RFC 2549, April 1, 1999, http://tools.ietf.org/rfc/rfc2549.txt.
5. Brian Carpenter and Robert Hinden, "Adaptation of RFC 1149 for IPv6," RFC 6214, April 1, 2011, http://tools.ietf.org/rfc/rfc6214.txt.
6. Bergen Linux Group, "The informal report from the RFC 1149 event," http://www.blug.linux.no/rfc1149/writeup.html.
7. Lisa Zyga, "Carrier Pigeon Faster Than Broadband Internet," *Phys.org*, September 11, 2009, http://phys.org/news171883994.html.
8. Nate Anderson, "What's faster than rural Internet uploads? Carrier pigeons," *Ars Technica*, September 16, 2010, http://arstechnica.com/tech-policy/2010/09/carrier-pigeons-beat-rural-internet-upload-speeds/.
9. Declan McCullagh, "How bin Laden evaded the NSA: Sneakernet," CNN, May 13, 2011, http://news.cnet.com/8301-31921_3-20062755-281.html.
10. Rigsum Sheran Collection, http://www.rigsum-it.com/research/projects/sherig/.
11. Reporters Without Borders, "North Korea: Frontiers of Censorship," October 2011, http://en.rsf.org/IMG/pdf/rsf_north-korea_2011.pdf; and Nick Farrell, "Cubans face off government with USB sticks," *Tech Eye*, March 12, 2013, http://news.techeye.net/security/cubans-face-off-government-with-usb-sticks.



LOOKING AHEAD

Rob Faris & Rebekah Heacock

The essays collected in this report echo a familiar narrative about Internet and society: digital technologies enable new forms of human interaction that disrupt existing political, social, and economic systems. Some of this disruption is good, and some bad. Public institutions, particularly legislative and formal regulatory mechanisms, have struggled to keep up with the rapid pace of change; companies and citizens have proven to be far more nimble in leveraging the affordances of digital communication and exploiting new opportunities. Although this narrative glosses over many important details—some of which are addressed earlier in this report—as a general premise, it tends to hold true. The ongoing legislative efforts around the world to create a coherent and enforceable framework for regulating online activity have shown modest success; meanwhile, private ordering plays a major role in digital affairs.

Many of the concerns over Internet policy and practice over the past two decades have focused on the nature and scale of content regulations by governments, such as the blocking of websites and social media platforms, and the appropriateness of different legal mechanisms for regulating online activity. This debate shows no signs of abating. Political pressure for restricting online content continues to be powerful, whether from civil society concerned with harmful activity online or from governments that are intent on consolidating power, though strong coalitions have emerged to resist proposals for greater Internet controls. In countries with a reliable adherence to the rule of law and robust civil liberties protections, the past two decades of debates over controlling Internet activity have commonly resulted in an uncomfortable balance of speech protections that leave much harmful speech unimpeded and fail to fully address security concerns. In more repressive environments, civil society activity has been suppressed without evidence of any corollary gains in terms of security or reduction of harmful speech.

Revelations regarding state surveillance have shifted the political landscape over the past year, and questions regarding the ramifications of and responses to this surveillance are likely to dominate Internet policy discussions into the foreseeable future, along with related questions of security and privacy. We appear to be entering a new stage in the debates over Internet policy based on the awkward realization that democratic governments that have promoted an open Internet also have been engaged in extensive surveillance, outside of the public scrutiny and with few political constraints, and that these surveillance programs likely represent a serious threat to the open Internet. This may mark the beginning of a major rethinking of the familiar narratives and allegiances in the debate over maintaining an open and connected Internet, with the United States at the center of the controversy. Although it is too soon to understand the full implications of these changes, they appear to have introduced a crisis of trust in the evolving Internet governance institutions and a growing rejection of the status quo and current distribution of power. Governments around the world have reacted to the surveillance revelations with a strong call to reduce the influence of the United States in managing the core infrastructure of the Internet. This provides political support to those countries that have pushed for a greater role for the ITU in Internet governance. The signatories of the Montevideo Statement on the Future of Internet Cooperation, including ICANN, ISOC, IETF, W3C, and several registries, called

for "accelerating the globalization of ICANN and IANA functions, towards an environment in which all stakeholders, including all governments, participate on an equal footing," which implies a lesser US role in these matters, although without suggesting an increase in the role of the ITU.

A growing fear is that failing to strike a new deal on state surveillance may lead to greater Balkanization if countries use this as a rationale for erecting greater walls around their sovereign space. More scrutiny is already being paid to international data flows and routing patterns, and the location of servers and data hosting will likely garner even more attention in the coming months.

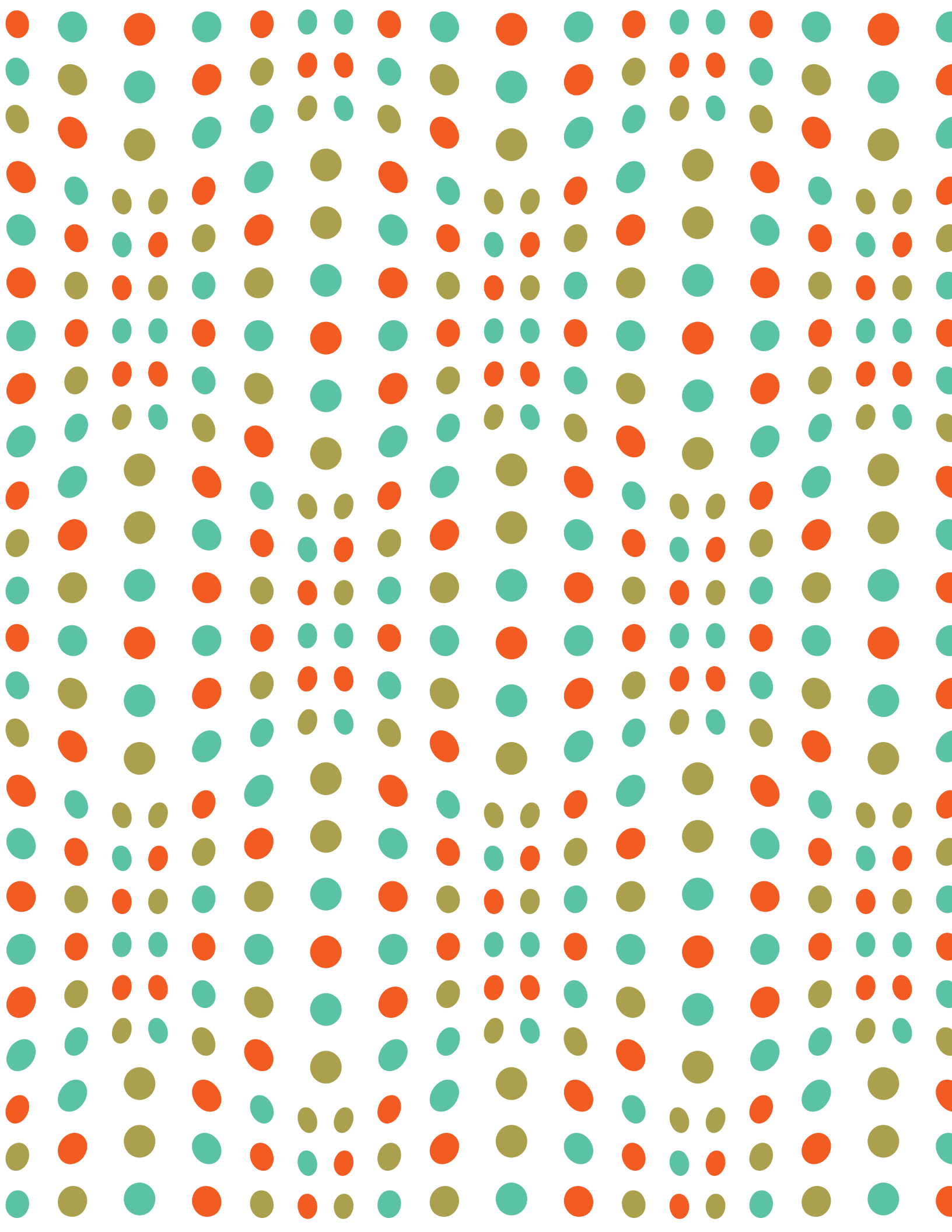
The general consensus is that the surveillance and information acquisition capabilities of governments are outpacing commercial and civil society efforts to secure personal communication online. This is true of the United States, China, Russia, and every other country that invests in state surveillance. A central question for the coming years will be whether a new bargain can be reached over the extent, means, and governance of state surveillance, both within and across national borders. As in prior policy questions, this plays out in both the political and technological realms. The political questions center on the viability of legal and institutional mechanisms to limit state surveillance. The veil of secrecy that ensconces state surveillance forms a formidable obstacle to attempts to limit the scope of government activity and promote transparency and accountability.

The battles over surveillance are being waged not only at the political and legal level but also by technologists, some working to better secure digital communication networks against unwanted snooping, and others cracking into these networks. Rather than seeking to define rules and regulations through legal and political channels, this battle is less constrained by laws and political processes, is more adversarial in nature, and is taking place largely out of public view—through tapping into submarine cables, gathering up telephone records, and hacking into private communication channels. Reforming the political and governance structures that operate state surveillance programs can and should be part of any solution. However, if the lessons of the past carry into the future, it will be the advances in the technologies of privacy and surveillance that define the limits of surveillance. An open question is whether surveillance-resistant tools are developed and deployed that will restore a widely accepted balance between state surveillance and private communication. Technology companies have a strong incentive to improve the sense of security among their users and to restore faith in their commitment to protect users from excessive surveillance. There is also renewed impetus to develop non-commercial and open source tools to secure online security and privacy.

Traditionally, cybersecurity and surveillance have not been strongly linked in policy discussions, and have been often presented as complementary: the notion that spying on one's enemies will help in securing digital networks from attack. This logic is inverted when a country turns the attention of its surveillance program to its own citizens. The technologies and tools that help to secure companies and citizens from unauthorized intrusions and cyberattacks also make state surveillance more difficult, and efforts to diminish these security measures make citizens and corporations more vulnerable to malicious attacks. Although far from a foregone conclusion, the current prominence of state surveillance issues could shift the framing of national debates around cybersecurity from a narrative of warring cyber armies to more broadly securing personal communication on digital networks from all potential attackers.

Protecting privacy online, whether from governments, companies, or other users, is of growing concern, and state surveillance is compounding a growing uneasiness regarding the acquisition, use, and distribution of personal information by private sector companies. Moreover, the ability of the state to collect information on people is supported by private sector data collection and the willingness of users to share information in private, semi-public, and public spaces online. This is a structural issue that runs deep into economic and social foundations of the Internet. A vast number of Internet users have offered up personal information to companies in quasi-consensual relationships in exchange for free access to social media, social networking, search, email, mobile applications, and a host of other online services. The monetization of this data in turn finances and maintains the Internet that entertains and enthralls these users. Crafting a new bargain over privacy and individual data seems both overdue and somehow more difficult by the minute. Any deal must work within or around the market and technological structures that define today's digital infrastructure. One question is whether Internet users may be willing to pay for more of the services they use in exchange for greater privacy protections. An alternative question is whether stronger legal mandates for protecting privacy online will imperil innovation in online consumer services.

Potentially lost in the debates over privacy, security, and surveillance, is the fact that access to information plays a critical role in human development, governance, and economic growth across all sectors, including health, education, energy, agriculture, and transportation. As the actions of governments, companies, and citizens shift the balance of privacy, surveillance, and security online, whether by technological, political, legal, or market-based means, important public policy questions lie in the balance.



BY THE NUMBERS

Number of new websites created per minute in 2013: 571.

Number of new domains registered: 70.

Number of photos posted to Tumblr: 20,000.

Number of new tweets: 278,000.

Of the top 100 most followed accounts on Twitter, the number that are musicians: 54.

Number that are tech companies: 7.

Number that are television show hosts: 7.

Number that are Brazilian soccer players: 3.

Number that are Kardashians: 3.

Number that are affiliated with One Direction: 6.

(Number of musicians in One Direction: 5.)

Speed reached by Li-Fi, a Wi-Fi alternative that transmits data by rapidly switching tiny light bulbs on and off: 10 Gbit/second.

Percentage of current Iranian cabinet members who maintain Facebook pages, despite the country's Facebook ban: 100.

Percentage by which traffic to adult entertainment website PornHub decreased in Chicago after the Chicago Blackhawks won the final game of the Stanley Cup: 19.

Percentage by which it increased in Boston, home of the Bruins (who, sadly, lost): 21.

Actors whose fan websites were defaced in the last year by Syrian Electronic Army hackers: Johnny Depp, Ben Affleck, Brad Pitt.

Among the terms censored on Chinese microblogging platform Sina Weibo this year: "hair bacon."

Number of copyright takedown requests Google received per second in September 2011: 0.29.

In September 2013: 8.76.

Size of English-language Wikipedia, in printed volumes, as of late 2013: 1930.

Of French-language Wikipedia: 469.

Vietnamese: 342.

Romanian: 40.

By the Numbers: Sources

"What happens online in 60 seconds?," Qmee, July 24, 2013, http://blog.qmee.com/qmee-online-in-60-seconds/.

"Twitter top 100: most followers," Twitter Counter, http://twittercounter.com/pages/100 (accessed October 29, 2013).

James Vincent, "Li-Fi revolution: internet connections using light bulbs are 250 times faster than broadband," The Independent, October 28, 2013, http://www.independent.co.uk/news/science/lifi-revolution-internet-connections-using-light-bulbs-are-250-times-faster-than-broadband-8909320.html.

Robert Tait, "Hassan Rouhani's cabinet open Facebook accounts," The Telegraph, September 9, 2013, http://www.telegraph.co.uk/news/worldnews/middleeast/iran/10296861/Hassan-Rouhanis-cabinet-open-Facebook-accounts.html.

Brian Stubits, "Chart: Boston turns to porn after Game 6 loss in Stanley Cup Final," CBSSports, June 25, 2013, http://www.cbssports.com/nhl/eye-on-hockey/22524719/study-boston-turns-to-porn-after-game-6-loss-in-stanley-cup-final.

Jason Q. Ng., Blocked on Weibo: What Gets Suppressed on China's Version of Twitter (And Why), (New York City: The New Press, 2013).

AFP, "China employs 2 million analysts to monitor web activity," RT, October 6, 2013, http://rt.com/news/china-internet-opinion-analysts-788/.

Google Transparency Report, "Requests to Remove Content: Due to copyright," http://www.google.com/transparencyreport/removals/copyright/?hl=en.

"Wikipedia: size in volumes," http://en.wikipedia.org/wiki/Wikipedia:Size_in_volumes.

"Modèle:Wikipédia sur papier," http://fr.wikipedia.org/wiki/Modèle:Wikipédia_sur_papier.

"Thành viên: Mxn/T□ sách," http://http://vi.wikipedia.org/wiki/Thành_viên:Mxn/T□_sách.

"Utilizator: Strainu/biblioteca," http://ro.wikipedia.org/wiki/Utilizator:Strainu/biblioteca.

CONTRIBUTORS

Christopher T. Bavitz is Managing Director of Harvard Law School's Cyberlaw Clinic, based at Harvard's Berkman Center for Internet & Society, and a Clinical Instructor and Lecturer on Law at HLS.

Ryan Budish is a fellow at the Berkman Center for Internet & Society and the Project Director of Herdict, which uses crowdsourcing to present a real-time view of Internet accessibility around the world. Prior to arriving at Harvard, he was an associate at the law firm of Covington & Burling LLP, in Washington, DC.

Sandra Cortesi is a Fellow at the Berkman Center for Internet & Society and the Director of Youth and Media. At Youth and Media, Sandra works closely with talented young people and lead researchers in the field as they look into innovative ways to approach social challenges in the digital world, including the production and exchange of digital media, youth development in social networking, and digital citizenship.

Masashi Crete-Nishihata is research manager for the Citizen Lab, at the Munk School of Global Affairs, University of Toronto. His research focuses on information controls (e.g., Internet censorship and surveillance) and their affect on human rights and international relations. Recent publications include work on multidisciplinary approaches to studying Internet censorship, global governance and the spread of information controls, and information security research ethics.

Ron Deibert is Professor of Political Science, and Director of the Canada Centre for Global Security Studies and the Citizen Lab at the Munk School of Global Affairs, University of Toronto. He is a co-founder and a principal investigator of the OpenNet Initiative and Information Warfare Monitor projects.

Bruce Etling is a Fellow at the Berkman Center for Internet & Society and doctoral student at the University of Oxford who contributes to Berkman's Internet Monitor, Media Cloud, and Internet Robustness projects. His research focuses on the impact of the Internet on collective action in democratic and hybrid regimes.

Robert Faris is the Research Director at the Berkman Center for Internet & Society. His recent research includes Internet content regulation, state censorship and surveillance practices, broadband and infrastructure policy, and the interaction of new media, online speech, and government regulation of the Internet and political processes.

Urs Gasser is the Executive Director of the Berkman Center for Internet & Society at Harvard University and a Professor of Practice at Harvard Law School. He is a visiting professor at the University of St. Gallen (Switzerland) and at KEIO University (Japan), and he teaches at Fudan University School of Management (China). Urs Gasser serves as a trustee on the board of the NEXA Center for Internet & Society at the University of Torino and on the board of the Research Center for Information Law at the University of St. Gallen, and is a member of the International Advisory Board of the Alexander von Humboldt Institute for Internet and Society in Berlin. He is a Fellow at the Gruter Institute for Law and Behavioral Research.

Bryan Han is a Harvard Law School student; he was enrolled in the Harvard Law School's Cyberlaw Clinic during the 2013 spring semester.

Rebekah Heacock is a Senior Project Manager at the Berkman Center for Internet & Society, where she manages a suite of projects related to access to information issues, including Internet Monitor and the OpenNet Initiative. She previously co-directed the Global Voices Technology for Transparency Network.

Jeff Hermes is the Director of the Digital Media Law Project at the Berkman Center for Internet & Society. He received his JD degree from Harvard Law School in 1997. Prior to joining the Berkman Center, Jeff assisted a wide array of clients in First Amendment, media, intellectual property and Internet law issues as a partner in the litigation practice of Brown Rudnick LLP and later as counsel to Hermes, Netburn, O'Connor & Spearing, P.C. in Boston.

Malavika Jayaram is a Fellow at the Berkman Center for Internet & Society, focusing on privacy, identity and free expression, especially in the context of India's biometric ID project. A practicing lawyer and a Fellow at the Centre for Internet and Society, Bangalore, she is the author of the India chapter for the Data Protection & Privacy volume in the Getting the Deal Done series. She is one of ten Indian lawyers in The International Who's Who of Internet e-Commerce & Data Protection Lawyers directory. In August 2013, she was voted one of India's leading lawyers—one of only 8 women to be featured in the "40 under 45" survey conducted by Law Business Research, London.

John Kelly is the Founder and Chief Scientist of Morningside Analytics, which discovers and monitors online networks that form around particular ideas. He previously co-directed the Interactive Design Lab at Columbia's Graduate School of Journalism.

Priya Kumar is a graduate student at the University of Michigan School of Information. Her self-designed curriculum in data storytelling incorporates data analysis, design, and policy work to learn how to glean insight from data and present it in compelling ways. Her research interests include digital privacy and online freedom of expression.

Ronaldo Lemos is the director of the Rio Institute for Technology and Society and a professor at the Rio de Janeiro State University's Law School. He is also a visiting scholar at the MIT Media Lab.

Colin M. Maclay is the Director of the Digital Initiative at Harvard Business School and a long-time Berkmaniac. His research, teaching, and practice lies at the intersections of new technologies, business models, institutions, and policy, and involves diverse sectors, disciplines, and modes. He serves on the founding board of the Global Network Initiative.

Viktor Mayer-Schönberger is Professor of Internet Governance and Regulation at the Oxford Internet Institute / Oxford University. He is also a faculty affiliate of the Belfer Center of Science and International Affairs at Harvard University.

Helmi Noman is a Senior Researcher at the Citizen Lab, Munk School of Global Affairs, University of Toronto and a Research Affiliate at the Berkman Center for Internet & Society. His research explores the impact of information and communication technologies on Arab information societies and how the use of the Internet defies the social and political structures in the region.

David R. O'Brien joined the Berkman Center for Internet & Society staff as a project coordinator in February 2011. David has been contributing legal and policy research to a number of Berkman projects and publications since 2009, including the Digital Media Law Project, Global Network Initiative, the Law Lab, the ICANN Accountability and Transparency review process, the Privacy Tools for Sharing Research Data project, the Cloud Computing Initiative, and Cybersecurity, among others.

Molly Sauter is a PhD student in Communication Studies at McGill University in Montreal. She holds a masters degree in Comparative Media Studies from MIT, and is a research affiliate at the Berkman Center for Internet & Society and the Center for Civic Media at the MIT Media Lab.

Bruce Schneier is an internationally renowned security technologist. He is a fellow at the Berkman Center for Internet & Society, a program fellow at the New America Foundation's Open Technology Institute, a board member of the Electronic Frontier Foundation, and an advisory board member of the Electronic Privacy Information Center.

Wolfgang Schulz is a professor at the Faculty of Law at the University of Hamburg on Media Law, Public Law and Legal Theory. He is also Director of the Hans-Bredow-Institut in Hamburg and of the Humboldt Institut for Internet and Society, Berlin. His main fields of research are media and Internet governance, comparative media law and policy, and freedom of communication.

Andy Sellars is the Berkman Center for Internet & Society's Corydon B. Dunham First Amendment Fellow and the Assistant Director of the Digital Media Law Project. He studies Internet free speech and intellectual property matters, and helps run the DMLP's pro bono referral clinic for online journalism ventures and digital media creators.

Ashkan Soltani is an independent researcher and consultant focused on privacy, security, and behavioral economics. His research examines the prevalence of online tracking and exposes practices designed to circumvent consumer privacy choices. Ashkan works to help journalists understand the technical nature and capability of various commercial and government surveillances. He has previously served as staff technologist in the Division of Privacy and Identity Protection at the Federal Trade Commission, worked as the primary technical consultant on the Wall Street Journal's "What They Know" investigative series, and is currently working with the Washington Post on their coverage of the NSA.

Dalia Topelson is a Clinical Instructor at Harvard Law School's Cyberlaw Clinic, based at Harvard's Berkman Center for Internet & Society. She is also a Lecturer on Law and co-teaches the Practical Lawyering in Cyberspace seminar with Christopher Bavitz. Dalia has concentrated her legal practice on intellectual property and media law, particularly in the areas of technology, media, privacy and digital content. Prior to joining Harvard Law School, Dalia worked as in-house counsel at Amazon.com, and as an associate at the New York law offices of Weil, Gotshal & Manges and DLA Piper LLP.

Rex Troumbley is a PhD candidate in the Department of Political Science at the University of Hawaii at Manoa. His dissertation research focuses on how taboo language (swearing, profanity, etc.) becomes subject to political and cultural governance. Lately his research has focused on how taboo language is regulated by digital technologies.

Zeynep Tufekci is an assistant professor at the University of North Carolina, Chapel Hill at at the School of Information and Library Science (SILS) with an affiliate appointment in the Department of Sociology. She is also a faculty associate at the Berkman Center and a fellow at Princeton's Center for Information Technology Policy. Her research revolves around the interaction between technology and social, cultural, and political dynamics.

Mark Wu is an Assistant Professor of Law at Harvard Law School and a Director of the Berkman Center for Internet & Society. His work focuses on international trade and international intellectual property matters. He has served as the Director for Intellectual Property in the Office of the US Trade Representative, an engagement manager for McKinsey & Co., and an economist and operations officer for the World Bank in China.

Jonathan Zittrain is Professor of Law at Harvard Law School and the Harvard Kennedy School of Government, Professor of Computer Science at the Harvard School of Engineering and Applied Sciences, and co-founder of the Berkman Center for Internet & Society. His research interests include battles for control of digital property and content, cryptography, electronic privacy, the roles of intermediaries within Internet architecture, human computing, and the useful and unobtrusive deployment of technology in education.