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.

> ***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

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.

> ***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.

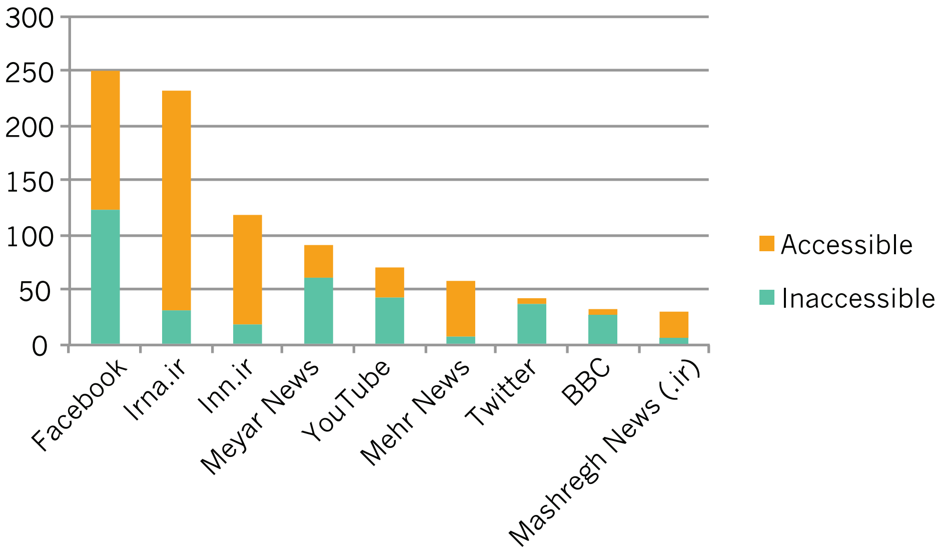

Figure 1: Herdict reports from Iran (select sites): June 1-July 1, 2013

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.

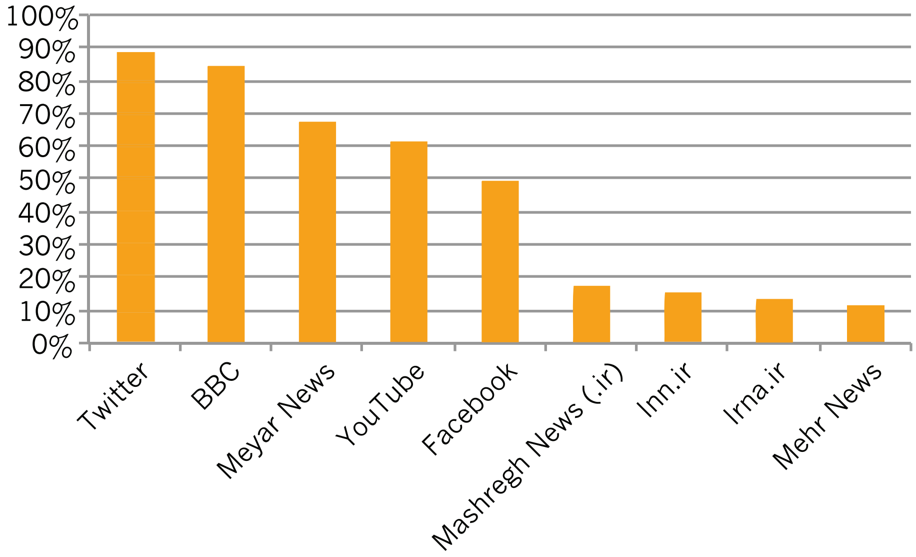

Figure 2: Percentage of Herdict reports indicating site inaccessible in Iran: June 1-July 1, 2013

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#.UlXcgmSifWo.

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.