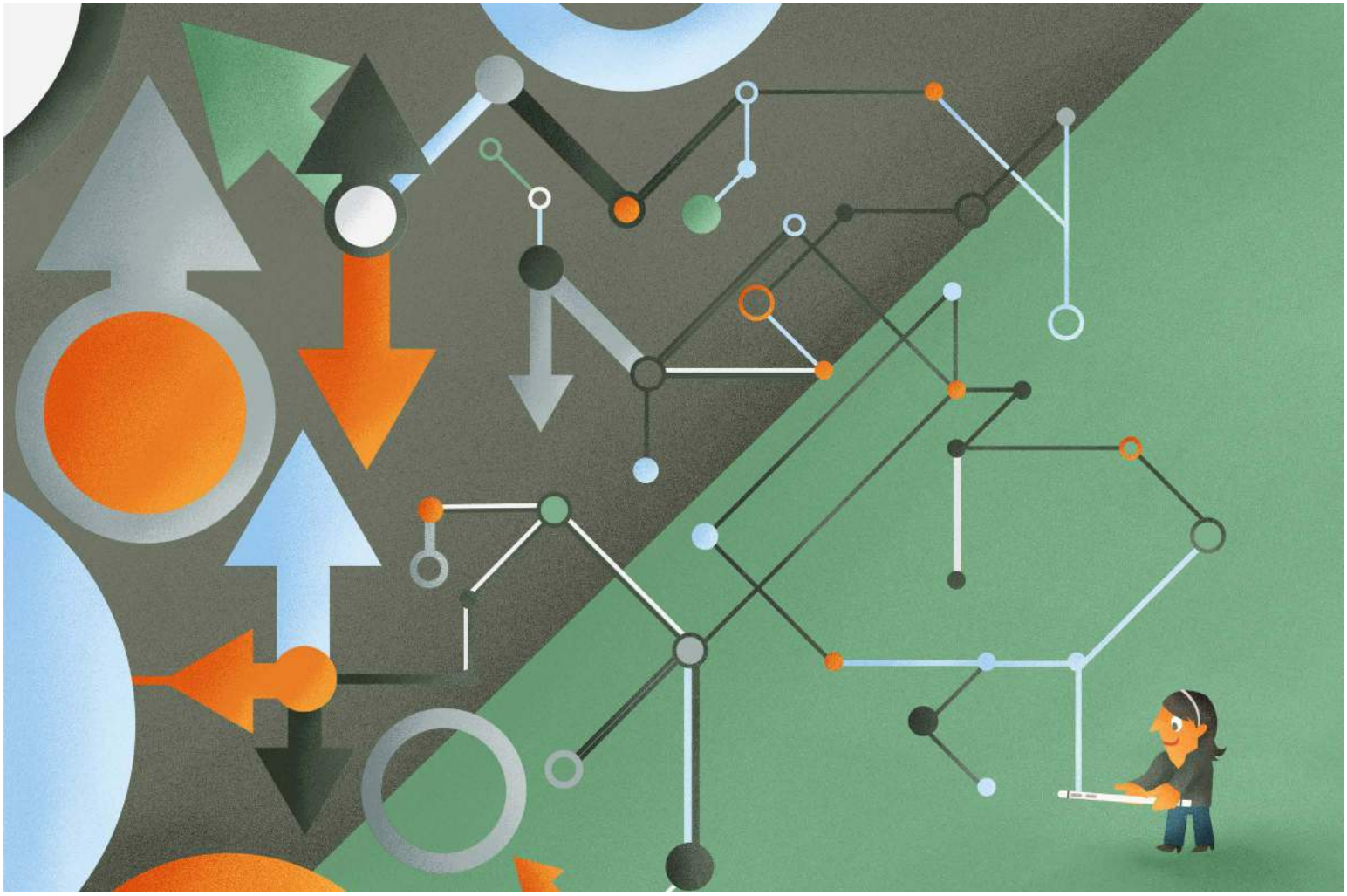
Toward a New Approach to Data Protection in the Big Data Era

INTERNET MONITOR

INTERNET MONITOR 2014

Reflections on the Digital World



With contributions from: ANA AZURMENDI • CHRISTOPHER T. BAVITZ • SUSAN BENESCH • EDUARDO BERTONI
ELLERY BIDDLE • WILLOW BRUGH • MONICA BULGER • NEAL COHEN • TIM DAVIES • ADRIENNE DEBIGARE
PRIMAVERA DE FILIPPI • ANDY ELLIS • SANDS FISH • ROBERT FARIS • NATHAN FREITAS
URS GASSER • REBEKAH HEACOCK JONES • ALISON HEAD • MALAVIKA JAYARAM • ETHAN KATSH
VIVEK KRISHNAMURTHY • JAMES LOSEY • ALESSANDRO MANTELERO • HELMI NOMAN • DAVID R. O'BRIEN
DALIA OTHMAN • JIOU PARK • JONATHON W. PENNEY • SHAWN POWERS • ORNA RABINOVICH-EINY
JORDI RODRIGUEZ VIRGILI • DAVID SANGOKOYA • CHARO SADABA • ANDREW SELLARS
HASIT SHAH • STEFAAN G. VERHULST • CLARENCE WARDELL
SARA M. WATSON • ROLF WEBER • JONATHAN ZITTRAIN

Berkman
The Berkman Center for Internet & Society
at Harvard University

ACKNOWLEDGEMENTS

The existence of this report is entirely the result of the dedicated and persistent effort of an outstanding team. First, we give thanks to our contributing authors, who generously shared both their time and their thoughtful reflections on the past year of digital activity. We are grateful to Bruce Etling and Helmi Noman for their valuable recommendations on the report as a whole, and to John Palfrey for providing the original inspiration for the Internet Monitor project.

We wish to extend our gratitude in particular to Robert Faris, who guided and developed this publication as Berkman's Research Director, and to Rebekah Heacock Jones, who managed the evolution and production of this report and provided extensive research, analytic, and editorial support. We also thank Adrienne Debigare and Jiou Park for additional editorial support, Dan Jones for design and layout, and Gretchen Weber for communications 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 second annual report of the Internet Monitor project at the Berkman Center for Internet & Society at Harvard University. As with the inaugural report, this year's edition is a collaborative effort of the extended Berkman community. *Internet Monitor 2014: Reflections on the Digital World* includes nearly three dozen contributions from friends and colleagues around the world that highlight and discuss some of the most compelling events and trends in the digitally networked environment over the past year.

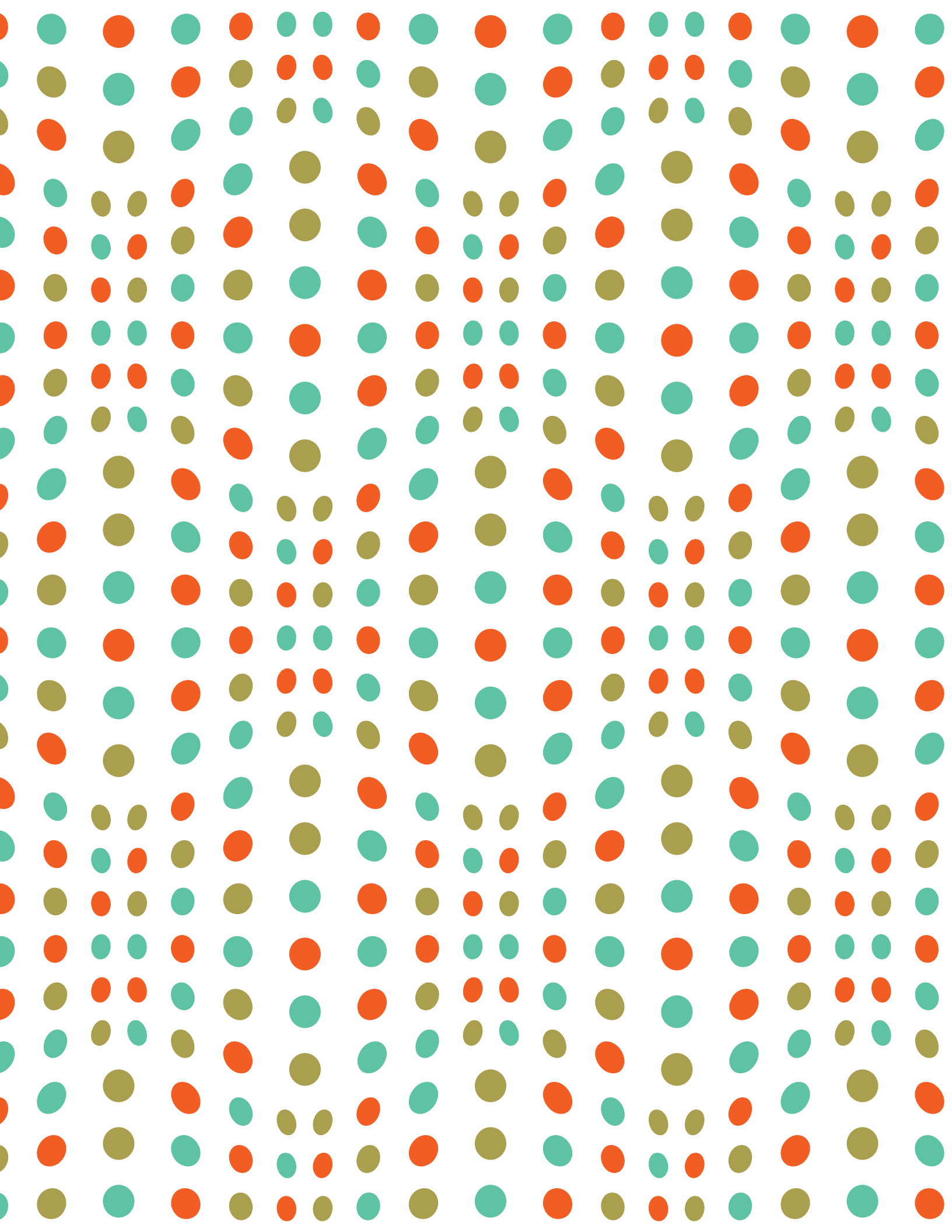
The result, intended for a general interest audience, brings together reflection and analysis on a broad range of issues and regions—from an examination of Europe's "right to be forgotten" to a review of the current state of mobile security to an exploration of a new wave of movements attempting to counter hate speech online—and offers it up for debate and discussion. Our goal remains not to provide a definitive assessment of the "state of the Internet" but rather to provide a rich compendium of commentary on the year's developments with respect to the online space.

Last year's report examined the dynamics of Internet controls and online activity through the actions of government, corporations, and civil society. We focus this year on the interplay between technological platforms and policy; growing tensions between protecting personal privacy and using big data for social good; the implications of digital communications tools for public discourse and collective action; and current debates around the future of Internet governance.

The report reflects the diversity of ideas and input the Internet Monitor project seeks to invite. Some of the contributions are descriptive; others prescriptive. Some contain purely factual observations; others offer personal opinion. In addition to those in traditional essay format, contributions this year include a speculative fiction story exploring what our increasingly data-driven world might bring, a selection of "visual thinking" illustrations that accompany a number of essays, a "Year in Review" timeline that highlights many of the year's most fascinating Internet-related news stories (and an interactive version of which is available at thenetmonitor.org), and a slightly tongue-in-cheek "By the Numbers" section that offers a look at the year's important digital statistics. We believe that each contribution offers insights, and hope they 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



BY THE NUMBERS

Date on which the number of domain names on the Internet is estimated to have crossed the one billion mark: September 17, 2014.

Number of the world's languages with "no detectable live online presence," based on research conducted at the Hungarian Academy of Sciences: 6541.

Number of new tweets per minute in 2013: 278,000.

In 2014: 433,000.

Of the top 100 most followed accounts on Twitter, the number that are Americans: 66.

Number that are Bollywood actors: 2.

Final date of operation for @everyword, a Twitter account launched in November 2007 to tweet every word in the English language: June 7, 2014.

Final tweet: "étui."

Third most retweeted tweet: "ugh."

Selection of things the media has claimed Twitter has "revolutionized" since its launch in July 2006: social media, the world, politics, education, the face of ballet in NYC, the way Snoop Dog makes music, children, old people.

Search terms more common in US states that rank highly in terms of economic, educational, and health outcomes: "holiday greetings," "baby massage," and half a dozen terms related to digital cameras.

Search terms in the lowest-ranked states: "diabetic diet," "antichrist," "38 revolver."

Number of days it would have taken the entire world to do the ALS Ice Bucket Challenge this summer, assuming everyone had been nominated and no one had declined: 35.

Number of daily active Facebook users, on average: 864 million.

Percentage of those users that are outside the US and Canada: 82.2.

Year in which dead people on Facebook are predicted to outnumber the living, assuming the site's user base continues to grow: 2130.

Percentage by which mobile traffic to news websites dropped during a 19-minute Facebook outage in August: 8.5.

Percentage by which desktop traffic increased: 3.5.

Previous upper limit of YouTube's view counter, before Psy's "Gangnam Style" exceeded the counter's 32-bit storage maximum: 2,147,483,647.

New upper limit: 9,223,372,036,854,775,808.

Number of views "Gangnam Style" has as of the date of this publication: 2,166,174,341.

Number of views the authors of this publication contributed while editing this piece: 3 4.

Percentage of Iranian young people reported to use proxy servers to circumvent online censorship: 69.3.

Number of public comments the US Federal Communications Commission received in response to its controversial net neutrality proposal: 3.7 million.

Percentage of those comments opposed to net neutrality, based on an initial analysis: <1.

Number of those comments, based on an initial analysis, that used identical suggested text from the Battle for Net Neutrality campaign site: 105,320.

Meters of accuracy within which a Florida State University research project can estimate where a given photo of a cat was taken: 7.8.

By the Numbers: Sources

Caitlin Dewey, "There are now officially a billion Web sites on the Internet (we think)," Washington Post, September 22, 2014, http://www.washingtonpost.com/news/the-intersect/wp/2014/09/22/there-are-now-officially-a-billion-web-sites-on-the-internet-we-think/.

András Kornai, "Digital Language Death," PLOS, October 22, 2014, http://www.plosone.org/article/info%3Adoi%2F10.1371%2Fjournal.pone.0077056#s7.

"Online in 60 seconds [Infographic] – A Year Later," Qmee, July 8, 2014, http://blog.qmee.com/online-in-60-seconds-infographic-a-year-later/.

"Twitter Top 100 Most Followers," Twitter Counter, http://twittercounter.com/pages/100.

Katherine Rosman, "Everyword, the Twitter Feed of Every Single Word, Is Shutting Down," Wall Street Journal, June 3, 2014, http://blogs.wsj.com/digits/2014/06/03/the-twitter-feed-of-every-single-word-is-shutting-down/.

everyword (@everyword), Twitter account, https://twitter.com/everyword.

everyword (@everyword), My Top Tweet, https://mytoptweet.com/?u=everyword.

Ben Dreyfuss, "Happy Birthday, Twitter! Here Are 50 Things the Media Says You've Revolutionized.," Mother Jones, July 15, 2014, http://www.motherjones.com/mixed-media/2014/07/happy-birthday-twitter-here-are-50-things-media-says-youve-revolutionized.

David Leonhart, "In One America, Guns and Diet. In the Other, Cameras and 'Zoolander.'," New York Times: The Upshot, August 18, 2014, http://www.nytimes.com/2014/08/19/upshot/inequality-and-web-search-trends.html?_r=0&abt=0002&abg=0.

Rhett Allain, "How Long Would It Take the Whole World to Do the Ice Bucket Challenge?," Wired, August 19, 2014, http://www.wired.com/2014/08/how-long-would-it-take-the-whole-world-to-do-the-ice-bucket-challenge/.

"Company Info," Facebook, http://newsroom.fb.com/company-info/.

Randall Munroe, "Facebook of the Dead," what if?, October 29, 2013, https://what-if.xkcd.com/69/.

Sam Kirkland, "Chartbeat: Mobile traffic dropped 8.5 percent during Friday's Facebook outage," Poynter, August 4, 2014, http://www.poynter.org/news/mediawire/261405/chartbeat-mobile-traffic-dropped-8-5-percent-during-fridays-facebook-outage/.

"Gangnam Style music video 'broke' YouTube view limit," BBC, December 4, 2014, http://www.bbc.com/news/world-asia-30288542.

"PSY - GANGNAM STYLE (강남스타일) M/V," YouTube video, 4:12, posted by "officialpsy,"July 15, 2012, https://www.youtube.com/watch?v=9bZkp7q19f0.

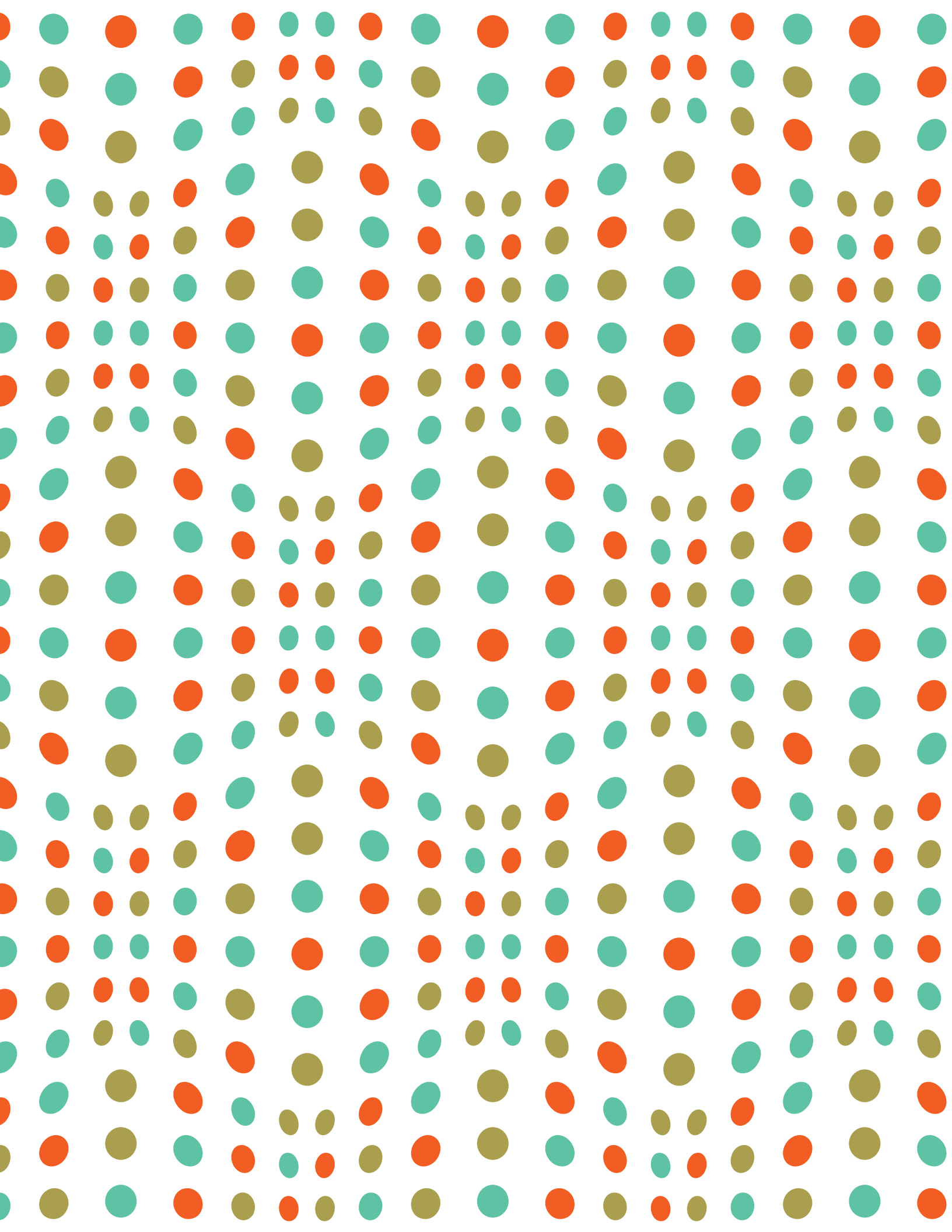
"70 Percent of Young Iranians Are Online Illegally," Daily Sabah, September 8, 2014, http://www.dailysabah.com/mid-east/2014/09/08/70-percent-of-young-iranians-are-online-illegally.

Jacob Kastrenakes, "FCC received a total of 3.7 million comments on net neutrality," The Verge, September 16, 2014, http://www.theverge.com/2014/9/16/6257887/fcc-net-neutrality-3-7-million-comments-made.

Bob Lannon and Andrew Pendleton, "What can we learn from 800,000 public comments on the FCC's net neutrality plan?," Sunlight Foundation Blog, September 2, 2014, http://sunlightfoundation.com/blog/2014/09/02/what-can-we-learn-from-800000-public-comments-on-the-fccs-net-neutrality-plan/.

Max Woolf, "The Data From Our Comments to the FCC About Net Neutrality," Minimaxir, August 8, 2014, http://minimaxir.com/2014/08/comments-about-comments/.

"About 'I Know Where Your Cat Lives,'" http://iknowwhereyourcatlives.com/about/.



2014 YEAR IN REVIEW

Adrienne Debigare, Rebekah Heacock Jones, and Jiou Park

An interactive version of this timeline with photos and video is available at http://brk.mn/2014yearinreview

January 2014

January 1: Palestinian poet Ashraf Fayadh is arrested for allegedly writing atheist poetry. Arab writers take to social media to voice their outrage for the arrest, claiming that Fayadh is being targeted for posting a video of religious police lashing a young man in public.[1]

January 4: Journalists and activists in Malaysia protest the indefinite government suspension of weekly news magazine The Heat. The groups attribute the suspension to an earlier article outlining the spending habits of the Prime Minister and his wife. The protest is named for red pencils that are broken in half to symbolize violence perpetrated against the media.[2]

January 8: Somalia's Al-Shabab militia uses Facebook to announce a ban on Internet access. The group gives telecom providers 15 days ultimatum to shut down services in the country.[3]

January 14: In what becomes one of the landmark court rulings of the year in the United States, the Court of Appeals rules that the FCC is not able to regulate broadband authorities as it does other "common carriers" like telephone companies. The decision reverses previously established FCC rules supporting net neutrality.[4]

January 16: The Ukrainian government responds to the Euromaidan protests by passing legislation that critics argue drastically limits freedom of expression. The bill comes after nearly two months of pro-European protests and is largely seen as a thinly veiled attempt at widespread censorship.[5]

January 17: President Obama delivers a long-awaited speech on NSA reform, focusing on the agency's phone record surveillance program. The reforms curtail the NSA's power to access information in the phone records database, but they do not address many of the agency's other activities.[6]

January 26: Chancellor Phyllis M. Wise disappoints students at the University of Illinois at Urbana-Champaign by deciding not to call a snow day despite very cold weather. Students start the hashtag #fuckphyllis and tweet "Asians and women aren't responsible for their actions," "Phyllis Wise is the Kim Jong Un of chancellors," and even more graphic attacks on Wise, who is Asian-American.[7]

February 2014

February 1: Ahead of the Olympic Games in Sochi, the Russian parliament passes legislation to limit free speech on the Internet by giving the Russian government the authority to censor any website or

social network that "'calls for participation in mass public events.'" [8]

February 5: The Turkish parliament adopts a new bill that allows the Telecommunications Communications Presidency (TIB) to block access to websites that violate privacy or contain "insulting" material without a court order.[9]

February 10: Glenn Greenwald, Laura Poitras, and Jeremy Scahill launch "The Intercept," a digital magazine dedicated to reporting on the Snowden revelations and to providing "aggressive and adversarial journalism." [10]

February 11: A massive DDoS attack, reaching 400 gigabits per second, hits EU and US based servers. The attack is 100 gigabits per second more powerful than the March 2013 Spamhaus attack, which was previously considered the biggest DDoS attack in history.[11]

February 11: Individuals, groups, and websites all over the world stage protests, hackathons, and online campaigns advocating against government mass surveillance as part of "The Day We Fight Back."[12]

February 12: Citizen Lab releases a report pinning cyber attacks against Ethiopian journalists living in the US on Ethiopian government hackers using commercial spyware developed in Italy.[13]

February 12: Senator Rand Paul files a lawsuit against President Obama and intelligence agency officials challenging the constitutionality of the NSA's bulk collection of American citizens' phone calls, joining a number of other plaintiffs including the ACLU.[14]

February 12: Anti-government protests leave at least three dead in Caracas, Venezuela. As the government begins to censor media broadcasts of the protests, citizens take to online space to report on the demonstrations. The government responds by blocking websites, denouncing use of social media, and throttling Internet connections.[15]

March 2014

March 12: For the first time in history, Reporters Without Borders names three governmental bodies in democracies in its annual "Enemies of the Internet" report: the US National Security Agency, UK Government Communications Headquarters, and Indian Centre for Development of Telematics.[16]

March 12: In the wake of Edward Snowden's surveillance leaks, the European Parliament passes sweeping legislation regarding data privacy and data handling.[17]

March 12: The world celebrates the 25th anniversary of the World Wide Web.[18]

March 13: In an attempt to prevent online bullying, harassment, and stalking, Singapore's Parliament unanimously passes The Protection from Harassment Act. Free expression activists express concerns

that the law may be used to limit free speech, including investigative journalism.[19]

March 13: The Russian Attorney General's Office issues a request to the country's mass media regulatory body to block four websites, including three news sites and the blog of activist Alexey Navalny. The government claims the sites "contain calls to illegal activity and participation in mass events that are conducted contrary to the established order."[20]

March 20: Turkey's telecommunications regulator reportedly bans Twitter as a means to apply a court ordered "protection measure." This ban comes after Turkish Prime Minister Recep Tayyip Erdogan responds to accusations of corruption posted on Twitter by promising to "wipe out" the site.[21]

March 25: Brazil's National Congress passes Marco Civil, the Brazilian Internet Bill of Rights. The bill is the first such piece of legislation in the world. Sir Tim Berners Lee issues a statement of support, crediting the bill with "help[ing] to usher in a new era—one where citizens' rights in every country around the world are protected by digital bills of rights."[22]

March 31: Gambian users of the chat app Viber report trouble accessing the app. Sources within Gambia's Telecommunications Company claim that the government is interfering with the service, while government officials claim telecoms operators, angry at the potential loss of business from those who prefer using Viber to making international calls, are responsible for the block.[23]

April 2014

April 1: Researchers discover a critical defect in OpenSSL, the open-source cryptographic software library used by about two-thirds of Web servers. This defect, dubbed "Heartbleed," allows attackers to recover private encryption keys, session cookies, and passwords without leaving traces in server logs.[24]

April 1: Mozambique's Council of Ministers submits a bill to Parliament that will criminalize texts, emails, and online posts that are "insulting" or "jeopardize the security of the state." The bill is in part a response to the country's 2010 "Bread Riots," protests against rising food and electricity costs that were organized largely via SMS.[25]

April 3: The European Parliament adopts a law on net neutrality that will prevent Internet service providers from discriminating against certain types of traffic based on the source and also end roaming fees across all EU countries.[26]

April 4: Twitter and YouTube are unblocked in Turkey following the Constitutional Court of Turkey's ruling that the bans violate free speech rights protected by the Turkish constitution.[27]

April 22: The #MarchaContraElSilencio (March Against Silence) kicks off a series of events in Mexico protesting the proposed Telecommunications Bill proposal. The bill enables telecommunications companies to "block, inhibit, or eliminate" communication services "at critical moments of public and

national security."[28]

April 23: NETmundial, the "Global Multistakeholder Meeting on the future of Internet Governance," takes place in Sao Pãolo, Brazil. Participants discuss principles of Internet governance and propose a roadmap for future development of the Internet governance ecosystem.[29]

May 2014

May 3: Digital activists in Bolivia dress as snails to protest slow Internet speeds across the country.[30]

May 8: A British man is sentenced to 8 weeks in jail for "sending a grossly offensive message via a public communications network" after tweeting his approval of the fatal stabbing of a teacher in Leeds, England. The man had also tweeted offensive remarks about Auschwitz and the Korean ferry disaster and racist comments about Muslim and Chinese people.[31]

May 11: Indonesia blocks Vimeo, Imgur, and Reddit amid government concerns about nudity on the sites.[32]

May 13: The European Court of Justice decides that individuals may ask search engines to delete links to information about them after a certain period of time. The "right to be forgotten" receives mixed reactions from freedom of information activists and information technology companies.[33]

May 13: Twenty months after YouTube is first blocked in Pakistan in response to the "Innocence of Muslims" film trailer, the High Court of Lahore rules that the site should be unblocked.[34]

May 19: Twitter blocks a pro-Ukrainian nationalist account from Twitter users whose location is set to Russia, citing the need to "reactively withhold access to certain content in a particular country from time to time" in cases where the company receives a "valid and properly scoped request from an authorized entity." Users whose location is set to another country are still able to see the account.[35]

May 20: Six Iranian youth are arrested for posting a cover video of Pharrell's "Happy" to YouTube and are forced to publicly "repent" on state television.[36]

May 20: In the wake of a military coup d'etat, Thailand's Army General imposes martial law. The military forbids both online and offline media from criticizing the army and demands that ISPs report to the new military-led "National Council for Peace and Order."[37]

May 22: China announces new state-mandated technology security standards as part of an inspection system that will affect many foreign technology products coming into the country.[38]

May 24: Serbian bloggers band together to speak out against the government's response to devastating floods earlier in the month, which included the arrest and detainment of social media users critical of the government's handling of the emergency.[39]

June 2014

June 5: Digital advocacy group Fight for the Future launches Reset the Net, a campaign to mark the one-year anniversary of the initial Snowden revelations. The campaign aims to push back against mass government surveillance by urging netizens to use encryption.[40]

June 5: Zelda Williams posts a "Dear Trolls" letter on Tumblr in response to hateful insults and attacks. On August 13, after her father Robin Williams commits suicide, Williams receives photographs made to look like his body, with text blaming her for his death. Horrified, Williams bows out of Twitter and other social media. Twitter suspends two accounts from which the images were sent, and thousands of people express sympathy for Williams. In September, she returns to tweeting.[41]

June 11: Egyptian pro-democracy blogger Alaa Abd El-Fattah and 24 other activists are sentenced in absentia to 15 years in jail, a joint LE 100,000 ($14,000) fine, and five years' surveillance for "organizing an unauthorized protest, attacking a police officer, and crowding a public space," among others.[42]

June 13: Just days before the civil referendum on voting rights for Hong Kong's Chief Executive elections, the online voting site hosting the referendum suffers massive DDoS attacks.[43]

June 13: In a landmark case, the Canadian Supreme Court rules that Internet users are entitled to the "reasonable" expectation of privacy and bars Internet service providers from disclosing users' personal information to law enforcement agents without a valid warrant.[44]

June 19: Blocks for several websites including Twitter, Skype, and Cubanet appear to be lifted in Cuba, only to return the following day. According to unconfirmed reports, the temporary access is due to a mistake by a government technician.[45]

June 26: Google begins removing search results in accordance with the May 2014 ruling by the Court of Justice of the European Union that search engines must comply with data protection laws allowing users to request that search results related to their name be removed (commonly known as the "right to be forgotten").[46]

June 27: African Union members approve the African Union Convention on Cyber Security and Personal Data Collection. The Convention covers a wide range of online activities, including electronic commerce, data protection, and cybercrime, and will lead to the enactment of national personal data protection laws if implemented.[47]

June 28: News breaks that Facebook, working with researchers at Cornell University, manipulated the content of users' news feeds to study the effects of positive and negative content on users' emotions. The news sparks a months-long debate on the ethics of social data research.[48]

July 2014

July 11: A 16-year-old girl named Jada speaks out after being drugged and raped at a party in Houston, Texas. Her rapist took photos and video of her—unconscious and lying awkwardly on the floor—and shared them on social media. Other teens begin uploading pictures of themselves in the same pose with the hashtag "#jadapose." Jada later posts a photo of herself with her fist in the air and her own hashtag: "#IAmJada." Supporters work to "take back" the meme, posting similar photos of themselves in solidarity with Jada.[49]

July 15: The UK's House of Commons passes a controversial law giving law enforcement access to citizen's phone and data records. The law, which is fast-tracked through Parliament after an April 2014 European Court of Justice ruling that revoked existing data retention powers, is widely criticized by privacy advocates.[50]

July 15: Investigative reporting by Radio Free Europe/Radio Liberty reveals that the daughters of Azerbaijani president Ilham Aliyev are the owners of two of the country's three telecoms. The information confirms that the Aliyev family controls 75% of the country's mobile market, including mobile Internet; activists raise concerns about the family's capabilities to monitor communications and online activity.[51]

July 16: Anne Sophie Leclere, a candidate for France's Front National right-wing party, is sentenced to nine months in jail for posting a photograph of a baby monkey on Facebook with the caption "at 18 months" next to a photograph of France's Minister of Justice, Christiane Taubira, with the caption "now." Taubira, who is black, endures other racist depictions both online and offline. Leclere is also fined 5,000 Euros and removed from the party.[52]

July 18: A growing number of Vietnamese activists find themselves unable to log in to Facebook after the government's online army, called "opinion shapers," uses Facebook's "report abuse" system to target the accounts for suspension.[53]

July 22: Spain passes a new law that gives publishers the right to seek payment from websites that link to their content with a "meaningful" description of said work. For those who don't pay, fines can reach 300,000 Euro ($372,000). The law, dubbed the "Google tax" by Spanish media, does not apply to social media sites but is otherwise vague, prompting concerns from bloggers, news sites, and other online publishers.[54]

July 23: The draft text of Tunisia's proposed cybercrime law is leaked. Critics claim the draft presents numerous threats to Internet progress in the country, including multiple restrictions on content that is contrary to "good morals."[55]

July 31: Russian Prime Minister Dmitry Medvedev signs a decree expanding the Kremlin's Internet surveillance program, which previously applied only to Internet service providers, to reach online social networks and all websites that allow people to message each other.[56]

August 2014

August 1: Russia's "Bill on Bloggers" comes into force, requiring all blogs with more than 3,000 daily readers to register with the state watchdog Roskomnadzor and authors to disclose their real identity. Authors must also comply with a set of restrictions including refraining from using obscene language, verifying information before publishing it, and abstaining from releasing reports containing slander or hate speech.[57]

August 6: Spyware company FinFisher is targeted by an anti-surveillance hacker who releases 40GB worth of client lists, source code, and more, aiming to expose links between the British-German company and governments in Bahrain and Pakistan.[58]

August 8: Iran's Ministry of Culture and Islamic Guidance announces that all news websites must obtain licenses from the Ministry's press supervisory board. According to the announcement, websites without government-issued licenses will be blocked nationwide.[59]

August 9: Amid an increasing crackdown on online speech, Chinese law enforcement authorities arrest four people on suspicion of spreading online rumors. 81 others are also detained or warned for similar or lesser offenses.[60]

August 11: Editors at Jezebel post an open letter to the leadership of Gawker Media, asking for help regarding gifs of rape and other violent misogyny that anonymous commenters are posting on their site and that editors are forced to remove manually. Gawker had ignored months of complaints, but responds quickly after the open letter.[61]

August 12: Ukraine's Parliament passes the first draft of a law that, if enacted, will allow the government to ban websites, printed materials, and TV and radio stations without a court order in order to protect national security.[62]

August 16: Video game developer Zoe Quinn's ex-boyfriend publishes a blog post implying that Quinn had exchanged sex for positive reviews of her recent game, Depression Quest. The post provokes a vitriolic campaign against Quinn that quickly morphs into a broader crusade against alleged corruption in games journalism. The movement, labeled #GamerGate, involves considerable abuse and harassment—including rape and death threats—of female developers and game critics.[63]

August 25: The Intercept publishes documents from the Snowden leaks showing that the National Security Agency is providing more than 850 billion records including emails, phone calls, and online chats to nearly two dozen US government agencies through a search engine called ICREACH.[64]

August 25: Over sixty Reddit users post a letter to the site's leadership titled, "We have a racist user problem and reddit won't take action." The letter calls out Reddit's inaction in response to "barrages" of "hateful, racist" posts and sparks a broad discussion of hate speech in the online community, which has over 170 million members.[65]

August 31: Over 500 private photos of female celebrities, including many nude photos, are posted to 4chan and widely circulated online. The photos were obtained from the owners' iCloud accounts, prompting speculation about the security of the Apple service. Apple denies that the leak resulted from a breach in the company's system, blaming a "very targeted attack on user names, passwords and security questions."[66]

September 2014

September 1: A Lebanese blogger leaks a copy of a memo from the country's Minister of Telecommunications ordering ISPs to block six pornography sites. The order marks the first application of Lebanese laws outlawing pornography to online content.[67]

September 2: LinkedIn announces that it is reconsidering its approach to censorship of Chinese content. The site, which launched in China in February, has heavily filtered Chinese-language content both within and outside of the country, but is now considering making this content accessible to users outside of China.[68]

September 5: Investigative reporting by Global Voices Advocacy cross-references data from the August 2014 FinFisher leak and a German parliamentary inquiry to reveal that British-German company Gamma International has illegally exported surveillance technology to multiple countries, including those with histories of human rights abuse.[69]

September 8: The Turkish government introduces a proposal that will give the country's Telecommunications Directorate almost absolute power to surveill Internet users and censor online content without a court order.[70]

September 10: US Net Neutrality activists institute "Internet Slowdown Day," urging websites to display symbolic "loading" symbols and Internet users to contact Congress members to show support for an Open Internet.[71]

September 15: Google's tenth transparency report reveals a 150% surge in US government information requests since the company began publishing transparency data in 2009.[72]

September 15: The Intercept publishes an essay by Edward Snowden alleging that New Zealand's Prime Minister lied to the public when he denied that the government is conducting mass surveillance on New Zealand's citizens.[73]

September 15: Prominent Egyptian blogger Alaa Abd El Fattah is released on bail, after being convicted of "organizing an unauthorized protest outside the Shura Council in Cairo."[74]

September 16: The government of Laos approves a bill that prohibits content that "[undermines] peace, independence, sovereignty, unity and prosperity of the country" and creates a compulsory real

name policy for all social media networks.[75]

September 17: Apple announces that its newest mobile operating system will automatically encrypt iPhone data, removing its previous ability to unlock certain data in response to law enforcement requests and search warrants.[76]

September 27: Cyberattacks against independent media and citizen organizing platforms in Hong Kong escalate, taking the majority of pro-democracy content offline in Hong Kong for over a week. The attacks are in response to the Occupy Central movement, which is advocating for equal suffrage in Hong Kong.[77]

October 2014

October 1: Leading Bahraini activist Nabeel Rajab is arrested for posting a tweet alleging that the Bahraini government's security institutions are an "incubator" for militant group ISIS.[78]

October 6: The Digital Reader blog breaks the news that Adobe Digital Editions and PDF Reader are logging and sending vast amounts of user data, including the entire contents of users' libraries and exactly what they have read, back to Adobe via an unencrypted http pathway.[79]

October 7: Twitter officially files suit against the US federal government, alleging an infringement of the company's 1st Amendment rights and advocating for a "right to transparency" to publish a more granular report of government information requests.[80]

October 14: Thomas Schneider, deputy head of Swiss communications regulator Ofcom, is elected to the role of chairman to ICANN's influential Government Advisory Committee. Schneider is expected to play a large role in the development of ICANN as it works to fully privatize the Internet's domain name system.[81]

October 16: Wikileaks publishes a leaked draft of the Trans-Pacific Partnership detailing the Intellectual Property agreement that the 12 participating countries are negotiating. The agreement would enforce stricter copyright and patent laws among member countries.[82]

October 24: The Nigerian Senate approves the Cybercrime Bill, which has been in negotiations for over a decade. The bill is intended to bring Nigerian law in line with international standards governing ATM card and identity theft, child pornography, intellectual property, and other areas.[83]

October 31: The Hungarian government announces that it will abandon a proposed "Internet tax," which would have charged approximately 0.6 US dollars for every gigabyte of Internet traffic, after tens of thousands of citizens take to the streets to protest the proposal.[84]

November 2014

November 7: A joint law enforcement operation conducted between 16 European countries and the US arrests 17 people, including Blake Benthall, alleged operator of Silk Road 2.0. The raid shuts down over 400 websites running on the Tor network that are purportedly selling illegal items, including drugs and weapons.[85]

November 10: President Obama issues a statement calling on the FCC to "implement the strongest possible rules to protect net neutrality." The statement comes after a record 3.7 million public comments are submitted to the FCC in support of net neutrality.[86]

November 18: WhatsApp announces end-to-end encryption of text messages sent between Android users. The new security feature is the strongest of any major texting application, and prevents WhatsApp from decrypting messages in response to requests from law enforcement.[87]

November 20: DDoS attacks against Hong Kong websites Apple Daily and PopVote, which have been vocal supporters of the Occupy Central movement and universal suffrage for the Chief Executive elections, grow to over 500 gigabytes per second—the largest in history.[88]

November 25: A group led by Mozilla, Akamai, Cisco, and the Electronic Frontier Foundation announces plans for a free, automated, and open certificate authority intended to make the process of encryption easier for website owners. The initiative, called Let's Encrypt, aims to "encrypt the entire Web."[89]

November 27: Australian game reviewer Alanah Pearce posts on Twitter that in response to rape threats she's received on Facebook, she has begun contacting the mothers of those sending the threats. At least one mother responds positively, by making her son write an apology and talking to his school about online harassment.[90]

November 27: The European Parliament passes a nonbinding resolution to break up Google. The resolution is largely symbolic, but experts say it may increase pressure on the European Union's competition commissioner to bring antitrust charges against the company.[91]

December 2014

December 1: The US Supreme Court hears oral arguments in Elonis v. United States, the first case about online threats to reach the court. The case has the potential to change how threats made online are judged—according to the intent of the speaker or based on the impact on the listener—and, accordingly, prosecuted.[92]

December 1: Mozilla releases Firefox 34, which uses Yahoo!—instead of Google—as its default search engine for US users.[93]

December 4: Freedom House issues its 2014 "Freedom of the Net" report, which finds a marked decline in Internet freedom worldwide over the past year. The report points to new legislation limiting free speech and expanding government surveillance powers in over 40 countries as a key factor.[94]

December 4: North Korea denies involvement in a sophisticated cyberattack targeting Sony Pictures Entertainment. Hackers stole and published 40GB of data, including employee Social Security numbers and unreleased films, during the attack on November 24. The studio is developing a comedic film involving the fictional assassination of North Korean leader Kim Jong-Un.[95]

December 5: The UK's Investigatory Powers Tribunal finds that the country's mass surveillance systems do not violate the European Convention of Human Rights. The organizations that brought the case, including Amnesty UK and Privacy International, are expected to appeal the decision.[96]

December 9: Police in Sweden raided a server room belonging to file-sharing service Pirate Bay, seizing servers and computers and effectively shutting down the site and its forum, Suprbay.org. Pirate Bay was previously raided in 2006, and its co-founders were convicted of copyright violations in 2009.[97]

December 11: In response to a sustained online harassment campaign against a female colleague, the Tor project issues a statement of solidarity against online harassment and in support of the "women who work on Tor [who] are targeted, degraded, minimized and endure serious, frightening threats."[98]

December 11: Google announces it will shut down Google News in Spain and remove Spanish publishers from the service worldwide to avoid charges levied by a new law in Spain. The law requires news aggregators to pay licensing fees to publishers or face heavy fines.[99]

Sources

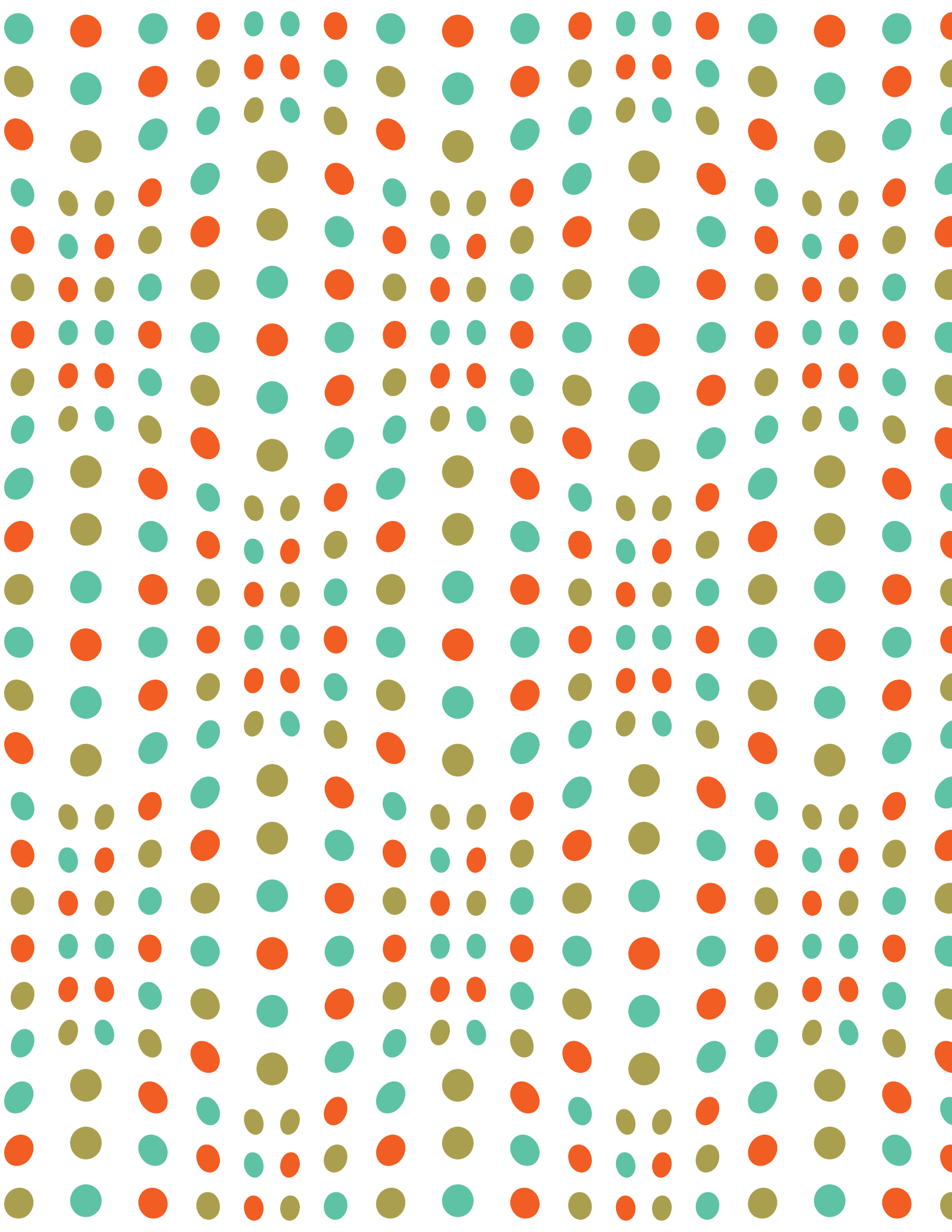
1. Global Voices, "Saudi Arabia Jails Palestinian Poet for 'Atheism and Long Hair,'" Global Voices Advocacy, January 28, 2014, http://advocacy.globalvoicesonline.org/2014/01/28/saudi-arabia-jails-palestinian-poet-for-atheism-and-long-hair/.
2. Mong Palatino, "'Red Pencil Protest' Demands Media Freedom in Malaysia," Global Voices Advocacy, January 13, 2014, http://advocacy.globalvoicesonline.org/2014/01/14/red-pencil-protest-demands-media-freedom-in-malaysia/.
3. "Al-Shabaab bans internet in Somalia, gives telecom companies 15-day ultimatum," Sabahi, January 9, 2014, http://sabahionline.com/en_GB/articles/hoa/articles/newsbriefs/2014/01/09/newsbrief-01.
4. Matthew Shaer, "In case of Verizon vs. FCC, is net neutrality the real loser?," Christian Science Monitor, January 15, 2014, http://www.csmonitor.com/Innovation/2014/0115/In-case-of-Verizon-vs.-FCC-is-net-neutrality-the-real-loser.
5. Global Voices, "Ukraine Stifles Freedom of Speech, Peaceful Protest With New Law," Global Voices Advocacy, January 20, 2014, http://advocacy.globalvoicesonline.org/2014/01/20/ukraine-stifles-freedom-of-speech-peaceful-protest-with-new-law/.
6. "Transcript of President Obama's Jan. 17 speech on NSA reforms," Washington Post, January 17, 2014, http://www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3-9556-4a4bf7bcbd84_story.html. See also: Brian Fung, "Everything you need to know about Obama's NSA reforms, in plain English," Washington Post, January 17, 2014, http://www.washingtonpost.com/blogs/the-switch/wp/2014/01/17/everything-you-need-to-know-about-obamas-nsa-reforms-in-plain-english/.
7. Scott Jaschik, "Snow Hate," Inside Higher Ed, January 28, 2014, https://www.insidehighered.com/news/2014/01/28/u-illinois-decision-keep-classes-going-leads-racist-and-sexist-twitter-attacks.
8. Mathias Bölinger, "Russia tightens Internet control ahead of Winter Olympic Games," DW, January 16, 2014, http://www.dw.de/russia-tightens-internet-control-ahead-of-winter-olympic-games/a-17367513.
9. "Turkish parliament adopts Internet censorship bill," Al Jazeera America, February 6, 2014, http://america.aljazeera.com/

articles/2014/2/6/turkish-parliamentadoptsinternetcensorshipbill.html.
10. Glenn Greenwald, Laura Poitras, and Jeremy Scahill, "Welcome to The Intercept," The Intercept, February 10, 2014, https://firstlook.org/theintercept/2014/02/10/welcome-intercept/.
11. "'Biggest ever'? Massive DDoS-attack hits EU, US," RT, February 11, 2014, http://rt.com/news/biggest-ddos-us-cloudflare-557/.
12. "February 11: The Internet Says No to Mass Surveillance," Global Voices Advocacy, February 10, 2014, http://advocacy.globalvoicesonline.org/2014/02/10/tomorrow-the-internet-says-no-to-mass-surveillance/.
13. Craig Timberg, "Foreign regimes use spyware against journalists, even in U.S.," Washington Post, February 11, 2014, http://www.washingtonpost.com/business/technology/foreign-regimes-use-spyware-against-journalists-even-in-us/2014/02/12/9501a20e-9043-11e3-84e1-27626c5ef5fb_story.html.
14. Charlie Savage, "Rand Paul Files Lawsuit Over N.S.A. Call Surveillance," New York Times, February 12, http://www.nytimes.com/2014/02/13/us/politics/rand-paul-files-lawsuit-over-nsa-call-surveillance.html.
15. Lorenzo Franceschi-Bicchierai, "Is Venezuela's Government Tightening its Grip on the Internet?," Mashable, February 20, 2014, http://mashable.com/2014/02/20/venezuela-social-media/.
16. "Enemies of the Internet 2014: Entities at the Heart of Censorship and Surveillance," Reporters Without Borders, March 11, 2014, http://en.rsf.org/enemies-of-the-internet-2014-11-03-2014,45985.html.
17. David Meyer, "Web firms face a strict new set of privacy rules in Europe—here's what to expect," Gigaom, March 12, 2014, https://gigaom.com/2014/03/12/web-firms-face-a-strict-new-set-of-privacy-rules-in-europe-heres-what-to-expect/.
18. Tim Berners-Lee, "Welcome to the Web's 25th Anniversary - a Message from Tim Berners-Lee," Web at 25, March 12, 2014, http://www.webat25.org/news/tbl-web25-welcome.
19. Neo Chai Chin, "Anti-harassment laws to fight 'social scourge,'" Today, March 14, 2014, http://www.todayonline.com/singapore/anti-harassment-laws-fight-social-scourge. See also: Mong Palatino, "Will Singapore's Anti-Harassment Law Curtail Free Speech?," Global Voices Advocacy, March 24, 2014, http://advocacy.globalvoicesonline.org/2014/03/24/will-singapore-anti-harassment-law-curtail-free-speech/.
20. "Russia Blocks Four Opposition Media Portals," Global Voices Advocacy, March 13, 2014, http://advocacy.globalvoicesonline.org/2014/03/13/russia-blocks-four-opposition-media-portals/.
21. "Twitter website 'blocked' in Turkey," BBC, March 20, 2014, http://www.bbc.com/news/world-europe-26677134.
22. "Brazilian Congress Approves Pioneer Bill of Rights for Internet Users," Global Voices Advocacy, March 26, 2014, http://advocacy.globalvoicesonline.org/2014/03/26/brazilian-congress-approves-pioneer-bill-of-rights-for-internet-users/.
23. Demba Kandeh, "Viber Chat App Blocked in The Gambia?," Global Voices Advocacy, March 31, 2014, http://advocacy.globalvoicesonline.org/2014/03/31/viber-chat-app-blocked-in-the-gambia/.
24. Dan Goodin, "Critical crypto bug in OpenSSL opens two-thirds of the Web to eavesdropping," Ars Technica, April 7, 2014, http://arstechnica.com/security/2014/04/critical-crypto-bug-in-openssl-opens-two-thirds-of-the-web-to-eavesdropping/.
25. Jornal @Verdade, "Mozambique Wants to Criminalize 'Insulting' Texts, Emails and Internet Posts," Global Voices Online, April 3, 2014, http://globalvoicesonline.org/2014/04/03/mozambique-wants-to-criminalize-insulting-texts-emails-and-internet-posts/.
26. Rebecca Chao, "European Parliament Adopts Law to Keep Internet Open," TechPresident, April 3, 2014, http://techpresident.com/news/wegov/24892/european-parliament-adopts-law-keep-internet-open.
27. "Turkish court lifts YouTube ban," Hurriyet Daily News, April 4, 2014, http://www.hurriyetdailynews.com/turkish-court-lifts-youtube-ban.aspx?pageID=238&nID=64544&NewsCatID=339.
28. Elizabeth, "#EPNvsInternet: Mass Campaign against Mexican Communications Bill," Global Voices Online, April 21, 2014, http://globalvoicesonline.org/2014/04/21/epnvsinternet-mass-campaign-against-mexican-communications-bill/.
29. "NETMundial Multistakeholder Statement," NETMundial, April 24, 2014, http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf. See also: NETMundial: Global Multistakeholder Meeting on the Future of Internet Governance, http://netmundial.br/; and NETMundial Initiative, https://www.netmundial.org/.
30. Eduardo Avila, "Bolivia's Internet at a Snail's Pace," Global Voices Online, May 6, 2014, http://globalvoicesonline.org/2014/05/06/bolivias-internet-at-a-snails-pace-2/.
31. Stevan Morris, "Man jailed for offensive Ann Maguire tweets," The Guardian, May 8, 2014, http://www.theguardian.com/uk-news/2014/may/08/man-jailed-offensive-ann-maguire-tweets.
32. Enricko Lukman, "Amid online porn crackdown, Vimeo, Reddit and Imgur are blocked in Indonesia," Tech In Asia, May 14, 2014, https://www.techinasia.com/online-porn-crackdown-vimeo-reddit-imgur-blocked-indonesia/.
33. David Streitfeld, "European Court Lets Users Erase Records on Web," New York Times, May 13, 2014, http://www.nytimes.com/2014/05/14/technology/google-should-erase-web-links-to-some-personal-data-europes-highest-court-says.html.
34. Nani Jansen, "Pakistan High Court Demands Unblocking of YouTube," Global Voices Advocacy, May 13, 2014, http://advocacy.globalvoicesonline.org/2014/05/13/pakistan-high-court-demands-unblocking-of-youtube/.
35. Brian Ries, "Twitter Blocks Pro-Ukrainian Political Account for Russian Users," Mashable, May 19, 2014, http://mashable.com/2014/05/19/twitter-blocks-account-russia/.
36. Robert Mackey, "Young Iranians Arrested for Being Too 'Happy in Tehran,'" New York Times: The Lede, May 20, 2014, http://thelede.blogs.nytimes.com/2014/05/20/young-iranians-arrested-for-being-happy-in-tehran.

37. "'I Can Feel Total Censorship in the Air': Internet Freedom Evaporates in Thailand," Global Voices Advocacy, May 30, 2014, http://advocacy.globalvoicesonline.org/2014/05/30/i-can-feel-total-censorship-in-the-air-internet-freedom-evaporates-in-thailand/.
38. Oiwan Lam, "China to Perform Security Inspections for Tech Products," Global Voices Advocacy, May 28, 2014, http://advocacy.globalvoicesonline.org/2014/05/28/china-to-perform-security-inspections-for-tech-products/.
39. Danica Radisic, "Serbian Bloggers Censored for Criticizing Flood Relief Efforts," Global Voices Advocacy, May 26, 2014, http://advocacy.globalvoicesonline.org/2014/05/26/serbian-bloggers-censored-for-criticizing-flood-relief-efforts/.
40. P. Nash Jenkins, "A Year After the Snowden Leaks, the Online Community Is Still Fuming," TIME, June 5, 2014, http://time.com/2825029/a-year-after-the-snowden-leaks-the-online-community-is-still-fuming/.
41. Caitlin Dewey, "Robin Williams's daughter Zelda driven off Twitter by vicious trolls," The Washington Post, August 13, 2014, http://www.washingtonpost.com/news/the-intersect/wp/2014/08/13/robin-williamss-daughter-zelda-driven-off-twitter-by-vicious-trolls/.
42. "Abd El Fattah, Shura Council defendants sentenced to 15 years in absentia," Mada Masr, June 11, 2014, http://www.madamasr.com/news/abd-el-fattah-shura-council-defendants-sentenced-15-years-absentia.
43. Oiwan Lam, "Hong Kong Voting Site Suffers Massive DDoS Attack Before Civil Referendum," Global Voices Advocacy, June 17, 2014, http://advocacy.globalvoicesonline.org/2014/06/17/hong-kong-voting-site-suffers-massive-ddos-attack-before-civil-referendum/.
44. Brid-Aine Parnell, "Top Canadian court: Cops need warrant to get names from ISPs," The Register, June 16, 2014, http://www.theregister.co.uk/2014/06/16/canada_supreme_court_privacy_isp_warrant/?mt=1413663903633.
45. Juan O. Tamayo, "Cuba ends censorship—NOT," Miami Herald, June 20, 2014, http://www.miamiherald.com/news/nation-world/world/americas/article1967398.html#.U6hYBYjVHgg.twitter.
46. David Meyer, "Google starts censoring search results in Europe due to privacy ruling," Gigaom, June 26, 2014, https://gigaom.com/2014/06/26/google-to-european-users-we-may-be-censoring-name-search-results-due-to-privacy-law/.
47. Ephraim Percy Kenyanito, "Africa moves towards a common cyber security legal framework," Access, June 2, 2014, https://www.accessnow.org/blog/2014/06/02/africa-moves-towards-a-common-cyber-security-legal-framework.
48. Gregory S. McNeal, "Facebook Manipulated User News Feeds To Create Emotional Responses," Forbes, June 28, 2014, http://www.forbes.com/sites/gregorymcneal/2014/06/28/facebook-manipulated-user-news-feeds-to-create-emotional-contagion/.
49. KHOU Staff, "16-year-old girl says her rape went viral: 'I'm just angry,'" KHOU, July 11, 2014, http://www.khou.com/story/local/2014/12/05/12664610/.
50. "Commons passes emergency data laws despite criticism," BBC, July 15, 2014, http://www.bbc.com/news/uk-28305309.
51. Khadija Ismayilova, "TeliaSonera's Behind-The-Scenes Connection To Azerbaijani President's Daughters," Radio Free Europe/Radio Liberty, July 15, 2014, http://www.rferl.org/content/teliasonera-azerbaijan-aliyev-corruption-investigation-occrp/25457907.html.
52. Peter Allen, "Member of French National Front jailed after she compared country's black justice minister to a monkey on Facebook," Daily Mail, July 16, 2014, http://www.dailymail.co.uk/news/article-2695076/Member-French-National-Front-jailed-compared-countrys-black-justice-minister-monkey-Facebook.html.
53. "Vietnamese Government 'Opinion Shapers' Target Activist Facebook Pages," Global Voices Advocacy, July 18, 2014, http://advocacy.globalvoicesonline.org/2014/07/18/vietnamese-government-opinion-shapers-target-activist-facebook-pages/.
54. Jason Koebler, "Spain Wants to Tax the Hyperlink," Motherboard, July 28, 2014, http://motherboard.vice.com/en_ca/read/spain-wants-to-tax-the-hyperlink.
55. Afef Abrougui, "Leaked Cybercrime Law Could Undo Tunisia's Pioneer Status on Internet Rights," Global Voices Advocacy, July 28, 2014, http://advocacy.globalvoicesonline.org/2014/07/29/leaked-cybercrime-law-could-undo-tunisias-pioneer-status-on-internet-rights/.
56. Sergey Kozlovsky, "Russia Just Doubled Its Internet Surveillance Program," Global Voices Online, August 15, 2014, http://globalvoicesonline.org/2014/08/15/russia-sorm-medvedev-social-networks-internet/.
57. "Legislative restrictions on popular bloggers come into force in Russia," RT, August 1, 2014, http://rt.com/politics/177248-russia-bloggers-law-restrictions/.
58. Violet Blue, "Top gov't spyware company hacked; Gamma's FinFisher leaked," ZD Net, August 6, 2014, http://www.zdnet.com/article/top-govt-spyware-company-hacked-gammas-finfisher-leaked/.
59. Mahsa Alimardani, "Iran Vows to Block All "Unlicensed" Websites," Global Voices Online, August 16, 2014, http://globalvoicesonline.org/2014/08/16/iran-vows-to-block-all-unlicensed-websites/.
60. "China Arrests Four for Spreading Online Rumors Amid Clampdown," Bloomberg News, August 9, 2014, http://www.bloomberg.com/news/2014-08-09/china-arrests-four-for-spreading-online-rumors-amid-clampdown.html.
61. Jezebel Staff, "We Have a Rape Gif Problem and Gawker Media Won't Do Anything About It," Jezebel, August 11, 2014, http://jezebel.com/we-have-a-rape-gif-problem-and-gawker-media-wont-do-any-1619384265.
62. Jonathan Keane, "New Law in Ukraine Would Curb Internet Freedom," VPN Creative, August 13, 2014, https://vpncreative.net/2014/08/13/law-ukraine-curb-internet-freedom/.
63. Sarah Kaplan, "With #GamerGate, the video-game industry's growing pains go viral," Washington Post, September 12,

2014, http://www.washingtonpost.com/news/morning-mix/wp/2014/09/12/with-gamergate-the-video-game-industrys-growing-pains-go-viral/.
64. Ryan Gallagher, "The Surveillance Engine: How the NSA Built its Own Secret Google," The Intercept, August 25, 2014, https://firstlook.org/theintercept/2014/08/25/icreach-nsa-cia-secret-google-crisscross-proton/.
65. Jason Abbruzzese, "Hate Speech Is Drowning Reddit and No One Can Stop It," Mashable, October 26, 2014, http://mashable.com/2014/10/26/reddit-hate-speech-moderation/.
66. Rich McCormick, "Hack leaks hundreds of nude celebrity photos," The Verge, September 1, 2014, http://www.theverge.com/2014/9/1/6092089/nude-celebrity-hack.
67. Nada Akl, "Lebanon Blocks Six Porn Sites, Sparks Fears of Further Censorship," Global Voices Advocacy, September 10, 2014, http://advocacy.globalvoicesonline.org/2014/09/10/lebanon-blocks-six-porn-sites-sparks-fears-of-further-censorship/.
68. Bruce Einhorn, "LinkedIn Weighs Less China Censorship. Can It Avoid Google's Fate?," Bloomberg BusinessWeek, September 3, 2014, http://www.businessweek.com/articles/2014-09-03/linkedin-wants-less-china-censorship-can-it-avoid-googles-fate.
69. Ben Wagner and Claudio Guarnieri, "EXCLUSIVE: German Companies Are Selling Unlicensed Surveillance Technologies to Human Rights Violators – and Making Millions," Global Voices Advocacy, September 5, 2014, http://advocacy.globalvoicesonline.org/2014/09/05/exclusive-german-companies-are-selling-unlicensed-surveillance-technologies-to-human-rights-violators-and-making-millions/.
70. "Turkey's telecom body given more power to monitor internet users," Hurriyet Daily News, September 9, 2014, http://www.hurriyetdailynews.com/turkeys-telecom-body-given-more-power-to-monitor-internet-users.aspx?pageID=238&nID=71480&NewsCatID=338.
71. "Sept. 10th is the Internet Slowdown," Battle for the Net, https://www.battleforthenet.com/sept10th/.
72. "Transparency Report: Government demands for user info have risen 150% over the last five years," Google Public Policy Blog, September 15, 2014, http://googlepublicpolicy.blogspot.com/2014/09/transparency-report-government-demands_15.html.
73. Edward Snowden, "Snowden: New Zealand's Prime Minister Isn't Telling the Truth About Mass Surveillance," The Intercept, September 15, 2014, https://firstlook.org/theintercept/2014/09/15/snowden-new-zealand-surveillance/.
74. Amira Al Hussaini, "Egyptian Blogger Alaa Abd El Fattah Released on Bail," Global Voices Online, September 15, 2014, http://globalvoicesonline.org/2014/09/15/egyptian-blogger-alaa-abd-el-fattah-released-on-bail/.
75. "New Laos web decree bans criticism of government policy – media," Reuters, September 23, 2014, http://uk.reuters.com/article/2014/09/23/uk-laos-internet-idUKKCN0HI0WN20140923.
76. Craig Timberg, "Apple will no longer unlock most iPhones, iPads for police, even with search warrants," Washington Post, September 18, 2014, http://www.washingtonpost.com/business/technology/2014/09/17/2612af58-3ed2-11e4-b03f-de718edeb92f_story.html.
77. Oiwan Lam, "The Invisible Violence of Cyber War in Hong Kong's Umbrella Revolution," Global Voices Online, October 6, 2014, http://globalvoicesonline.org/2014/10/06/the-invisible-violence-of-cyber-war-in-hong-kongs-umbrella-revolution/.
78. Noor Mattar, "Bahrain's Prominent Human Rights Activist Arrested for Criticizing Police Defectors Who Joined ISIS," Global Voices Online, October 1, 2014, http://globalvoicesonline.org/2014/10/01/bahrains-prominent-human-rights-activist-arrested-for-criticizing-police-defectors-who-joined-isis/.
79. Sean Gallagher, "Adobe's e-book reader sends your reading logs back to Adobe—in plain text [Updated]," Ars Technica, October 7, 2014, http://arstechnica.com/security/2014/10/adobes-e-book-reader-sends-your-reading-logs-back-to-adobe-in-plain-text/.
80. Ben Lee, "Taking the fight for #transparency to court," Twitter Blog, October 7, 2014, https://blog.twitter.com/2014/taking-the-fight-for-transparency-to-court.
81. "The GAC Elects New Chair and Vice-Chairs," ICANN Announcements, October 16, 2014, https://www.icann.org/news/announcement-3-2014-10-16-en.
82. Jeremy Malcom and Maira Sutton, "Latest TPP Leak Shows US Still Pushing Terrible DRM and Copyright Term Proposals—and New Threats Arise," Electronic Frontier Foundation, October 16, 2014, https://www.eff.org/deeplinks/2014/10/latest-tpp-leak-shows-us-still-pushing-terrible-drm-and-copyright-term-proposals.
83. Adam Oxford, "New Nigerian law means seven years for cybercrime," ZD Net, November 5, 2014, http://www.zdnet.com/article/new-nigerian-law-means-seven-years-for-cybercrime/.
84. Rick Lyman, "Hungary Drops Internet Tax Plan After Public Outcry," New York Times, October 31, 2014, http://www.nytimes.com/2014/11/01/world/europe/hungary-drops-internet-tax-plan-after-surge-of-protests.html.
85. Jane Wakefield, "Huge raid to shut down 400-plus dark net sites," BBC, November 7, 2014, http://www.bbc.com/news/technology-29950946.
86. Edward Wyatt, "Obama Asks F.C.C. to Adopt Tough Net Neutrality Rules," New York Times, November 10, 2014, http://www.nytimes.com/2014/11/11/technology/obama-net-neutrality-fcc.html.
87. Russell Brandom, "WhatsApp rolls out end-to-end encryption using TextSecure code," The Verge, November 18, 2014, http://www.theverge.com/2014/11/18/7239221/whatsapp-rolls-out-end-to-end-encryption-with-textsecure.
88. Parmy Olson, "The Largest Cyber Attack In History Has Been Hitting Hong Kong Sites," Forbes, November 20, 2014, http://www.forbes.com/sites/parmyolson/2014/11/20/the-largest-cyber-attack-in-history-has-been-hitting-hong-kong-

sites/.
89. Peter Eckersley, "Launching in 2015: A Certificate Authority to Encrypt the Entire Web," Electronic Frontier Foundation, November 18, 2014, https://www.eff.org/deeplinks/2014/11/certificate-authority-encrypt-entire-web.
90. "Troll's mum tells him to apologise after victim contacts her," BBC, December 2, 2014, http://www.bbc.co.uk/newsbeat/30290141.
91. James Kanter, "E.U. Parliament Passes Measure to Break Up Google in Symbolic Vote," New York Times, November 27, 2014, http://www.nytimes.com/2014/11/28/business/international/google-european-union.html.
92. Vauhini Vara, "The Nuances of Threats on Facebook," New Yorker, December 3, 2014, http://www.newyorker.com/news/news-desk/nuances-threat-facebook.
93. Owen Williams, "Mozilla releases Firefox 34, marking switch to Yahoo as default search engine," The Next Web, December 1, 2014, http://thenextweb.com/apps/2014/12/01/mozilla-releases-firefox-34-marking-switch-yahoo-default-search-engine/.
94. Doug Bernard, "Study: Governments Grow Bolder in Blocking Online Freedom," Voice of America, December 4, 2014, http://www.voanews.com/content/governments-grow-bolder-in-blocking-online-freedom-study-says/2545300.html.
95. Elise Hu, "North Korea's Cyber Skills Get Attention Amid Sony Hacking Mystery," NPR, December 4, 2014, http://www.npr.org/blogs/alltechconsidered/2014/12/04/368449855/north-koreas-cyber-skills-get-attention-amid-sony-hacking-mystery.
96. "GCHQ does not breach human rights, judges rule," BBC, December 5, 2014, http://www.bbc.com/news/uk-30345801.
97. Kim Zetter, "Pirate Bay Has Been Raided and Taken Down: Here's What We Know," Wired, December 9, 2014, http://www.wired.com/2014/12/pirate-bay-raided-taken-down/.
98. "Solidarity against online harassment," Tor, December 11, 2014, https://blog.torproject.org/blog/solidarity-against-online-harassment.
99. Justin Ellis, "Google News closes up shop in Spain," Nieman Lab, December 11, 2014, http://www.niemanlab.org/2014/12/google-news-closes-up-shop-in-spain/.



PLATFORMS AND POLICY

Robert Faris and Rebekah Heacock Jones

Digitally mediated communication and activity continue to collide with existing political, social, economic, and cultural structures in complex and fascinating ways. More and more of people's lives are moving into the digital realm. For some, there is little of their existence that is not either directly mediated through digital means or recorded by digital devices: sleep cycles; work history; health information; financial records; social networks; shopping culture; tastes in music, literature, and movies; home heating schedules; and preferences in romantic partners. Many years after the well-chronicled struggles of the music and media businesses, which continue today, the rapid success of 'sharing' economy platforms such as Uber and Airbnb are testament to the ongoing potential of digital platforms to invade markets long dominated by entrenched capital-intensive industries in unexpected ways. The reach of e-commerce giants, such as Alibaba and Amazon, continues to expand, while other sectors—energy, health, and education, for example—seem poised for dramatic changes enabled by digital platforms in the coming years.

The profusion of new services and apps available for consumers progresses unabated; the number of apps available for download in Google Play is approaching 1.5 million with iTunes close behind. Internet users continue to adopt newer services to communicate online, such as Instagram, Snapchat, Vine, or Yik Yak. Upset with Facebook's real name policy, instituted in September 2014, a vocal set of users moved to a newer social networking platform, Ello. None of this appears to threaten the ongoing dominance of a small number of large platforms, led by Google, Facebook, Twitter, and Amazon, which are helped along by a combination of network effects and economies of scale and scope. The Indie Web movement and other attempts to re-decentralize the Internet face an uphill battle.

Meanwhile, large swathes of the world are completely unconnected. While the number of people connected to the Internet approaches 3 billion, well over 4 billion are not connected. According to the ITU, 78 percent of households in developed countries have Internet access compared to 32 percent in developing countries, and just 5 percent in the least developed countries.[1] A major portion of the world is connected through low-bandwidth mobile devices with small keyboards and screens. The differences in experience, salience, opportunity, and impact of the Internet between highly connected and sparsely connected societies are enormous, in terms of access to locally relevant information, economic linkages, and social networks online.

Penetration rates and connectivity speeds continue to rise around the world, and in some regions, connectivity costs are falling. There is still a huge disparity in the affordability of the Internet, and much of the difference in penetration rates might be explained by this factor alone. For much of the developed world, access costs are less than 5 percent of household disposable income, even for lower income earners. In other countries, the cost of access can greatly exceed the 5 percent threshold and for lower income earners, the cost of access can be greater than household income.[2]

Several billion people now have the ability to find their way into our field of view and enthrall us, offend us, invade our privacy, steal our secrets, or make us fear for our lives. The potential for the

digitally connected to impact one another's lives, for better or worse, has expanded.

In last year's report, we highlighted a number of unsettled and contentious issues that are shaping the Internet. At the top of the list is the inherent perpetual difficulty in regulating online spaces. This continues to frustrate every government around the world, regardless of where their Internet policies and practices fall on the spectrum of open versus closed. Over the past decade or so, the core regulatory challenges have changed in degree but not in kind; issues of scale, jurisdiction, and attribution, which are tied to the ability to conduct surveillance, complicate any efforts to regulate online activity. The ability to identify individuals associated with online activity facilitates regulation whether in China or Canada, and mechanisms that allow individuals to cloak their identity or to take refuge outside of their government's jurisdiction reduce regulatory effectiveness. There is an awkward symmetry to this issue of regulatory efficacy: a central point of concern among those advocating for Internet freedom is over the ability of governments to inappropriately prevent content and ideas from circulating. On the other side of the coin, there are real concerns over the inability of regulators to prevent illicit or damaging content from circulating. The state of technology strongly influences these regulatory challenges, and determines in part how far governments and private companies can go to do good and bad. However, it is not true that technology always wins. And code alone does not set the boundaries for online behavior. Policy and law play an important role, and social norms and ethics do continue to influence online behavior. The battle for control of the Internet in the area of law, policy, and community standards is being fought atop the shifting sands of technology advances, some in favor of greater privacy and openness, while others more easily enable restrictions and surveillance.

The past year has not been good for Internet freedom in repressive regimes. Authoritarian governments continue to suppress Internet activity with the collection of tools at their disposal; they use content filters, cyberattacks, and surveillance systems to identify dissidents in conjunction with an array of legal and extralegal mechanisms to intimidate, discourage, and punish. Freedom House reported that the past year witnessed more arrests associated with Internet activity than in any other year.[3] This is deplorable and unsurprising, and likely reflects more political and social activism online in addition to the ongoing suppression of dissident voices. The arrest of six Zone9 bloggers in Ethiopia marked another ignoble milestone there.[4] In China, a large number of microbloggers were detained, evidently as a result of their popularity.[5] Political bloggers and online activists continue to be arrested in Vietnam, Gambia, Venezuela, Turkey, and the list goes on.

Internet filtering of political, religious, and social content continues to be most prevalent in the Middle East and parts of Asia. The number of countries with pervasive filtering systems has changed little in recent years, having reached an equilibrium point several years ago in which those that have the power to implement such a system have already done so. Pakistan introduced commercial mass filtering software to implement political, religious and social filtering in 2013.[6] Even Somalia, declared by some to be a failed state, has started using mass Internet filtering technology.[7] Filtering within countries varies over time to coincide with key political and social events such as elections and unrest. For example, the Russian parliament passed new legislation allowing for filtering just weeks before the 2014 Winter Olympic Games in Sochi;[8] Venezuela's government responded to political protests by blocking Internet users from sharing photos via Twitter and, reportedly, completely shut-

ting down Internet service in some parts of the country.[9]

China and Iran continue to stand out for their willingness to apply every available tool to suppress the spread of ideas and the formation of online communities. The hopes for a gradual opening of the Internet in Iran since Rouhani took office in 2013 have not come to fruition. The greatest change over the past year has been in Russia, which has assembled an array of legislation that would enable it to break off from the rest of the Internet in a manner similar to the Chinese.[10] A question for the coming year is whether Russia takes that next step, and if so, what the repercussions will be. Legislation passed in July and expected to take effect in September 2016 will require all online companies operating in Russia, whether domestic or international, to store data on local servers. Websites that fail to follow the new rules will be blocked.[11]

The government of Turkey continues to struggle with the social and political activities of a digitally connected citizenry, punctuated by the Gezi Park protests of 2013. Both Twitter and YouTube were blocked during February and March 2014 before court orders overturned the blocking orders. The passage of amendments to the country's Internet Law 5651 in February expanded the grounds for blocking websites to include infringements on privacy. Many interpreted this move to have been a response to information leaks related to government corruption.[12]

Journalists and Internet users living in areas controlled by militants in Syria and Iraq face serious challenges. Islamic State militants have killed journalists and activist Internet users who dare to post content perceived un-Islamic or not conforming to the militants' ideology.[13]

The incidence of cyberattacks continues to grow, combining a constantly evolving set of malware combined with attacks targeting individual users based on resource-intensive research and social engineering. In November 2014, DDoS attacks against pro-democracy websites in Hong Kong reached more than 500 gigabytes per second, the largest volume in history.[14] Doxing—the practice of compiling (through a mix of Internet research and hacking) and broadcasting personal information about someone—has affected a wide range of individuals, from female game developers and journalists targeted for their comments on the Gamergate controversy (most of whom also received rape and death threats)[15] to Ku Klux Klan members, whose identities and credit card information were published as part of an Anonymous campaign in response to the fatal shooting of Michael Brown in Ferguson, Missouri.[16]

Governments have employed crowdsourcing to go after political opponents. These 'electronic armies' advance state interests by taking down the online presence of political opponents and dissidents and by running defamation campaigns. The use of electronic armies is a new tactic that serves these regimes well by making the aggression against the political opponents look like popular movements; establishing attribution is often difficult, which helps governments to distance themselves from these activities. Amnesty International quoted a Saudi activist as saying that among the ways Saudi Arabia is silencing people online is the deployment of cyber armies that "give a false impression of the situation in Saudi Arabia to deceive people overseas" and depict activists as "atheists, infidels and agents who promote disobedience of the Ruler" and at the same time "praise the state and its efforts."[17]

While filters are put in place to limit the flow of information, authorities well understand that squashing ideas and arguments is both difficult and of secondary importance. It is the formation of networks that facilitate social mobilization that concerns them the most, and explains the focus on individual leaders and increased attention in times of potential instability. A lesson of the color revolutions, the Arab spring, and a growing number of digitally mediated social movements is that politically motivated and highly connected netizens can be rapidly transformed into street protesters. The hopes that liberation technologies might decisively turn the tide on authoritarian governments and undo the power of authoritarian regimes to quell popular uprisings have diminished over time. The dictator's dilemma—whether and how to allow the diffusion of communication technologies knowing that they are key to economic and social progress yet also empower civil society—is still relevant today, but may not be as sharp-edged as many had predicted.

In many countries, particularly those with stringent controls on traditional media, the ability to find and express alternative views on political and social issues is unquestionably enhanced by digital communication. The Internet can be a haven for those banned from openly participating in political activity. This greater autonomy also extends to participating in communities that promote ideas and lifestyles that are severely curtailed in offline spaces, such as non-traditional religious persuasions and sexual orientation, and the fight for women's rights. The willingness of authoritarian regimes to ignore or tolerate online behaviors that would be suppressed offline is being tested daily in many countries around the world.

The inclination and ability to control online intermediaries—including ISPs, telecommunications companies, mobile carriers, social media and social networking platforms, content hosts, app providers, and the like—continues to be the principal functional difference between those countries that infringe on digital human rights and those with a better record of protecting civil liberties online. Forcing intermediaries to cooperate with the government in removing and blocking content has been the foundation for Internet filtering regimes for almost two decades. The other key instrument—requiring intermediaries to surrender data on users—is employed by law enforcement everywhere. In some countries, communication infrastructure is directly controlled by the government, making access to data that much easier.

Private companies control a vast majority of the Internet's physical infrastructure and much of the software that rests on it, and hence play a profoundly influential role in defining online spaces. They serve as enthusiastic or reluctant agents of law enforcement mandates and at times as advocates for protecting users and a line of defense against governmental overreach. In repressive regimes, governments play the principal role in deciding what type of content is allowed to flourish online, for example by dictating which topics are used to populate filtering lists and takedown requests. Mass Internet filtering software made in Western countries continues to be implicated in state-mandated political, social, and religious filtering in the Middle East and most recently in Pakistan and Somalia.

In more open societies, governments are appropriately less involved in policing content. In its place, private ordering—the voluntary arrangements worked out by non-governmental actors—is the principal mechanism for shaping and constraining Internet activity. Terms of use govern the limits for

user behavior on the most prominent platforms, for example, keeping pornography and violence off of YouTube and Facebook. Enforcing such standards on private platforms—although not subject to the same procedural standard and accountability as one might expect in the legal system—is still subject to problems of scale and attribution. In the end, someone or something has to decide what comes down and what stays. The practical solution commonly adopted is a mix of crowdsourcing that allows users to flag offensive material, automated filters, and human review, which introduces mistakes in both overreach and underreach and results in the removal of innocuous material while leaving toxic content untouched. Accuracy and fairness do not scale well.

In open societies, the quest for balance between reining in damaging speech and protecting openness, civic rights, and freedom of expression continues to be hotly debated. The open recruiting of fighters in the West by militants in Syria and Iraq, most notably ISIS, has renewed calls by some for battling extremism online with tighter content restrictions. The United Kingdom has taken a particularly aggressive approach to fighting online extremism, removing over 15,000 of pieces of content in the first half of 2014. In June, UK government representatives met with the heads of Google, Facebook, Twitter, and Microsoft to discuss the removal of extremist content that is not technically illegal and the disclosure of user data related to those who post such content.[18] In cases where these companies have refused to disclose such data, the UK government has expressed outrage, criticizing them for "providing a safe haven for terrorists."[19] In early December, China passed new laws to combat religious extremism in the Xinjiang region, instituting fines for those who use the Internet or mobile phones to incite hatred.[20]

The incidence of hate speech, racism, misogyny, harassment, and threats of physical violence on the Internet has gained more attention in the press and policy discussions in the past year. It is difficult to ascertain whether the amount and severity of toxic speech online has increased over the past year. It does seem apparent that the calls for measures to rein in damaging speech have increased, leading many to reconsider whether a redrawing of the lines that protect free expression online are warranted. The coverage of incidents of revenge porn and leaking of private intimate photos of celebrities, which also draw in questions of online privacy and security, has raised similar calls for regulatory action to tighten regulations on online behavior and enforcement capacity. These questions fall at the intersection of political (what is the right balance between protecting freedom of expression online and protecting victims of malicious attacks online?), technical, and practical (what measures are best suited to addressing this issue and what are the collateral costs associated with them?).

Perhaps the most consequential decision on Internet content in recent years took place in May 2014, when the European Court of Justice issued a "right to be forgotten" ruling that forces search engines to remove links to material deemed to be "inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing at issue carried out by the operator of the search engine."[21] The stakes for individuals online are high if the first page of online search results represents "the ten things that define you."[22] This ruling offers a new foray into the application of notice and takedown regimes, similar to that used for the DMCA, which governs the removal of content based on the infringement of copyright. This system is scalable and problematic in many ways.

A bright spot for many in the past year was the passage of the Marco Civil da Internet in Brazil in the spring of 2014. Negotiated over several years with the involvement of civil society, government, and industry, the bill offers a broad codification of Internet rights including provisions to safeguard user rights to privacy, access to information, and free expression; safe harbor provisions that limit liability for intermediaries; and guidelines for net neutrality. The bill is remarkable not only for its novel articulation of Internet rights but also for the open public process that facilitated the creation of the law, which ultimately helped to overcome opposition to the bill and assure its passage. This precedent could set in motion other similar efforts to codify Internet rights as a counterbalance to measures to restrict activity, which are often crafted for noble reasons but can infringe upon and inhibit legitimate speech online.

The past year has also been eventful for net neutrality debates around the globe. In the addition to the passage of the Marco Civil in Brazil, the European Parliament passed strong net neutrality legislation in April 2014. In the United States, while the FCC decided how to respond to the deep divide between open Internet proponents and telecommunications companies over possible non-discrimination guidelines, President Obama came down decisively on the side of strong net neutrality provisions, calling on the FCC to "implement the strongest possible rules" to preserve an open Internet.23 Angela Merkel has taken a stance more closely aligned with industry in suggesting that a two-tiered system will better enable innovation: one "lane" for high priority traffic and one that resembles current conditions.[24]

The world continues to come to terms with the revelations of pervasive state surveillance. The reverberations are being felt in policy debates around the world: in proposed legislation, in company policies, in civil society mobilization efforts, and in a renewed focus on the development of better technology and tools. In some countries—Brazil and Russia, most notably—the response to these revelations has been to draft legislative proposals calling for the localization of data storage, raising fears over further balkanization of the Internet. Brazil ultimately bowed to pressure from technology companies and removed the data storage provision from Marco Civil,[25] while Russia, as noted above, continues to push on. In November, the United Nations passed a non-binding resolution, spearheaded by Brazil and Germany, calling on states to review their mass surveillance practices and protect the right to privacy.[26]

Public outcry against surveillance among civil society and Internet rights groups around the world continues. In the United States, the anti-surveillance campaigns organized in February around the banner The Day We Fight Back brought considerable attention to the issue. Organizers reported that 550,000 emails and 89,000 phone calls expressing opposition to broad-scale surveillance policies were delivered to US legislators.[27] Others noted that that the size and reach of the protests was smaller than the social mobilizations against SOPA and in favor of net neutrality legislation.[28] The legislation in the US to impose greater restrictions on dragnet surveillance has so far been unsuccessful.[29]

The technological responses to surveillance over the past year have been remarkable, adding to the many long-standing efforts by industry, non-profit organizations, and individuals to secure communi-

cation and privacy on the Internet and through mobile communications to protect against snooping governments, private sector data collection, and malicious hackers. Apple announced that data held on iPhones would be encrypted by default.[30] The popular messaging app, WhatsApp, introduced end-to-end encryption on communications using the app, such that the company would be unable to turn over the content of these messages to law enforcement requests.[31] Mozilla, in conjunction with the Tor Project and the Center for Democracy and Technology, launched the Polaris Privacy Initiative, which will offer new privacy features to the Firefox browser.[32] EFF, Mozilla, Cisco, Akamai, and researchers at the University of Michigan announced Let's Encrypt, a new certificate authority to help transition more web traffic to HTTPS.[33] While security concerns on the Internet still remain high, the response from law enforcement agencies to the recent moves by companies and non-profit organizations has ranged from negative to hyperbolic, with the director of British electronic intelligence agency GCHQ accusing American technology companies of being the "command-and-control networks of choice for terrorists and criminals."[34]

Governments have not in general supported overall security measures that would make it more difficult for government surveillance but also better protect users from other incursions into personal privacy and data security at the hands malicious hackers and corporate data breaches. As companies and civil society groups continue to develop and improve tools to protect user privacy and security, these technologies will be exported, adapted, and applied by users around the world. If they are successful, the next question is what political moves will be set into motion to respond.

Notes

1 International Telecommunication Union, "The World in 2014: ICT Facts and Figures," April 2014, http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2014-e.pdf.

2 International Telecommunication Union, Measuring the Information Society Report 2014, http://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2014/MIS2014_without_Annex_4.pdf. See Chart 4.1, "Fixed-telephone basket (left) and mobile-cellular basket (right), in PPP$, world and by level of development, 2008-2013," page 109. For more information on the cost of Internet access, see Internet Monitor's analysis of broadband pricing ("Sources: Price," http://thenetmonitor.org/sources), based on the international broadband service pricing dataset produced by Google Policy By the Numbers (Fei Xue, "International Broadband Pricing Study: Updated Dataset," March 20, 2014, Google: Policy By The Numbers, http://policybythenumbers.blogspot.com/2014/03/international-broadband-pricing-study.html). See also Alliance for an Affordable Internet, Affordability Report 2013, http://a4ai.org/affordability-report-2013/.

3 Freedom on the Net 2014, Freedom House, December 4, 2014, https://freedomhouse.org/report/freedom-net/freedom-net-2014#.VIXRG2TF9dU.

4 Endalk, "Six Members of Blogging Collective Arrested in Ethiopia," Global Voices Advocacy, April 26, 2014, http://advocacy.globalvoicesonline.org/2014/04/26/six-members-of-blogging-collective-arrested-in-ethiopia/.

5 Chris Buckley, "Crackdown on Bloggers is Mounted by China," New York Times, September 10, 2013, http://www.nytimes.com/2013/09/11/world/asia/china-cracks-down-on-online-opinion-makers.html?pagewanted=all&_r=0.

6 "O Pakistan, We Stand on Guard for Thee: An Analysis of Canada-based Netsweeper's Role in Pakistan's Censorship Regime," Citizen Lab, June 20, 2013, https://citizenlab.org/2013/06/o-pakistan/.

7 "Internet Filtering in a Failed State: The Case of Netsweeper in Somalia," Citizen Lab, February 20, 2014, https://citizenlab.org/2014/02/internet-filtering-failed-state-case-netsweeper-somalia/.

8 Mathias Bölinger, "Russia tightens Internet control ahead of Winter Olympic Games," DW, January 16, 2014, http://www.dw.de/russia-tightens-internet-control-ahead-of-winter-olympic-games/a-17367513.

9 Lorenzo Franceschi-Bicchierai, "Is Venezuela's Government Tightening its Grip on the Internet?," Mashable, February 20, 2014, http://mashable.com/2014/02/20/venezuela-social-media/.

10 Andrey Tselikov, "The Tightening Web of Russian Internet Regulation," Internet Monitor Special Report, November 2014, http://thenetmonitor.org/research/runet_regulation.

11 Adrien Henni, "New personal data storage law to affect both foreign and domestic players," Russia Beyond the Headlines, July 15, 2014, http://rbth.com/politics/2014/07/15/new_personal_data_storage_law_to_affect_both_foreign_and_domestic_pl_38209.html.

12 "Turkey: Internet Freedom, Rights in Sharp Decline," Human Rights Watch, September 2, 2014, http://www.hrw.org/

news/2014/09/02/turkey-internet-freedom-rights-sharp-decline.

13 "Islamic State militants kill two Iraq journalists," BBC, October 14, 2014, http://www.bbc.com/news/world-middle-east-29613783. See also: Raja Abdulrahim, "Islamic State killed human rights lawyer in Iraq, U.N. says," LA Times, September 25, 2014, http://www.latimes.com/world/middleeast/la-fg-iraq-islamic-state-kill-lawyer-20140925-story.html.

14 Parmy Olson, "The Largest Cyber Attack In History Has Been Hitting Hong Kong Sites," Forbes, November 20, 2014, http://www.forbes.com/sites/parmyolson/2014/11/20/the-largest-cyber-attack-in-history-has-been-hitting-hong-kong-sites/.

15 Soraya Nadia McDonald, "Gamergate targets Felicia Day after she expresses fear of being targeted," Washington Post, October 24, 2014, http://www.washingtonpost.com/news/morning-mix/wp/2014/10/24/gamergate-targets-felicia-day-after-she-expresses-fear-of-being-targeted/.

16 "Anonymous posts KKK leader's personal data online in ongoing war over Ferguson," RT, November 28, 2014, http://rt.com/usa/209875-anonymous-kkk-leader-dox/.

17 "7 ways Saudi Arabia is silencing people online," Amnesty International, December 6, 2014, http://www.amnesty.org/en/news/7-ways-saudi-arabia-silencing-people-online-2014-12-06.

18 Patrick Wintour, "Government reveals scale of online fight against jihadist propaganda," The Guardian, June 23, 2014, http://www.theguardian.com/world/2014/jun/23/jihadist-propaganda-government-youtube-british-muslims-isis. See also Jenny Gross, Lisa Fleisher, and Sam Schechner, "U.K. Seeks Help From Tech Firms in Combating Extremists Online," The Wall Street Journal, October 22, 2014, http://www.wsj.com/articles/u-k-seeks-help-from-tech-firms-in-combating-extremists-online-1414010650.

19 Sam Jones, Helen Warrell, and Conor Sullivan, "MPs slam Facebook in Lee Rigby case," Financial Times, November 25, 2014, http://www.ft.com/intl/cms/s/0/2e01225e-748c-11e4-8321-00144feabdc0.html?siteedition=uk#axzz3LJyDfo6P.

20 "Beijing passes laws to combat religious extremism in Xinjiang," Today Online, December 2, 2014, http://www.todayonline.com/chinaindia/china/beijing-passes-laws-combat-religious-extremism-xinjiang.

21 "An internet search engine operator is responsible for the processing that it carries out of personal data which appear on web pages published by third parties," Court of Justice of the European Union Press Release No 70/14, May 13, 2014, http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf.

22 Jonathan Zittrain, "The ten things that define you," Future of the Internet, May 15, 2014, http://blogs.law.harvard.edu/futureoftheinternet/2014/05/15/the-ten-things-that-define-you/.

23 "Net Neutrality: President Obama's Plan for a Free and Open Internet," http://www.whitehouse.gov/net-neutrality#section-read-the-presidents-statement.

24 Dante D'Orazio, "Angela Merkel argues against net neutrality, calls for special access fast lane," The Verge, December 6, 2014, http://www.theverge.com/2014/12/6/7345219/angela-merkel-argues-against-net-neutrality-calls-for-special-access.

25 Allison Grande, "Brazil Nixes Data Localization Mandate From Internet Bill," Law360, March 20, 2014, http://www.law360.com/articles/520198/brazil-nixes-data-localization-mandate-from-internet-bill.

26 Ben Quinn, "United Nations human rights committee resolves to protect privacy," The Guardian, November 25, 2014, http://www.theguardian.com/law/2014/nov/26/united-nations-human-rights-privacy-security.

27 "The Day We Fought Back: By the Numbers," https://thedaywefightback.org/the-results/.

28 Adi Robertson, "Not many of us actually fought on the Day We Fight Back," The Verge, February 13, 2014, http://www.theverge.com/2014/2/13/5408034/not-many-of-us-actually-fought-on-the-day-we-fight-back.

29 Kim Zetter, "Critical NSA Reform Bill Fails in the Senate," Wired, November 18, 2014, http://www.wired.com/2014/11/usa-freedom-act-fails-in-senate/.

30 Craig Timberg, "Apple will no longer unlock most iPhones, iPads for police, even with search warrants," Washington Post, September 18, 2014, http://www.washingtonpost.com/business/technology/2014/09/17/2612af58-3ed2-11e4-b03f-de718edeb92f_story.html.

31 Russell Brandom, "WhatsApp rolls out end-to-end encryption using TextSecure code," The Verge, November 18, 2014, http://www.theverge.com/2014/11/18/7239221/whatsapp-rolls-out-end-to-end-encryption-with-textsecure.

32 Denelle Dixon-Thayer, "Introducing Polaris Privacy Initiative to Accelerate User-focused Privacy Online," Mozilla Privacy Blog, November 10, 2014, https://blog.mozilla.org/privacy/2014/11/10/introducing-polaris-privacy-initiative-to-accelerate-user-focused-privacy-online/.

33 Peter Eckersley, "Launching in 2015: A Certificate Authority to Encrypt the Entire Web," Electronic Frontier Foundation, November 18, 2014, https://www.eff.org/deeplinks/2014/11/certificate-authority-encrypt-entire-web.

34 Alan Cowell and Mark Scott, "Top British Spy Warns of Terrorists' Use of Social Media," New York Times, November 4, 2014, http://www.nytimes.com/2014/11/05/world/europe/GCHQ-director-tech-companies-militants.html.

SOPA Lives: Copyright's Existing Power to Block Websites and "Break the Internet"

Andrew Sellars

It has been over four years since the bill later known as SOPA[1] was introduced in Congress, and nearly three years since SOPA was abandoned in a watershed moment for popular constitutionalism and online democratic participation.[2] SOPA has now become a four-letter word around Capitol Hill, invoked whenever a group wants Internet legislation to fail. But some of SOPA's most outrageous powers—the powers that allowed law enforcement to take down material without any meaningful judicial procedure by targeting DNS providers—didn't need SOPA to appear. They are already in the law. They have been used before in the name of copyright enforcement, and they sit waiting to be used again.

As several scholars at the time noted, SOPA's problems with freedom of expression were largely procedural in nature.[3] The bill created a system where private parties or the Attorney General could defund or take down online content without any court deciding, even preliminarily, that the content in question infringed copyright. This violates "First Amendment due process," a shorthand for a doctrine coming from a series of cases from 1960s-80s where the Supreme Court imposed strict limitations for governments attempting to seize or license the sale of material suspected to be obscene.[4] The effect of these rulings was to institute extra procedures that law enforcement must follow when seizing books, films, magazines, and other expressive material for its content: impartial judges make the call as to whether content is, in fact, unlawful, either before or immediately after the government seizes material; decisions about what content is unlawful are not made by agents in the field; and seizures done for the purpose of gathering evidence do not have the effect of stopping speech from reaching its audience until a court weighs in.[5] These are burdens that go beyond what law enforcement must normally do in order to seize evidence or contraband—as one court remarked, the standards and procedures for seizing unlawful speech are stricter than those for arresting unlawful speakers.[6]

And so whether or not the content on what SOPA called "foreign infringing sites" did violate copyright law, SOPA was wrong in suggesting the government could go about censoring it in the way that the bill contemplated.[7] This result is very much as it should be; the guard against prior restraints is the oldest and most treasured piece of the First Amendment mosaic, in place for very good reasons.[8] The substance of free speech would be lifeless without adequate procedures.

And yet, the powers contemplated in SOPA were not without precedent. Indeed, essentially the same powers had been used already. In a move that received nowhere near the attention SOPA received, federal law enforcement in 2010 and 2011 blocked websites at 24 domain names in the name of copyright enforcement in a program called "Operation In Our Sites."[9] The sites were largely described as "linking" sites that contained links to files stored on various cloud storage and "cyberlocker" sites, though several sites also contained blogs, forums, and other content.[10] No judge was ever involved to adjudicate the websites' criminality, even as a preliminary matter. No accommodation was made to ensure that speech would continue to reach its audience while illegality was determined. In short, the more stringent standards of "First Amendment due process" were nowhere to be found. All that it

took was a warrant, a statement before a magistrate showing that law enforcement had some cause to believe that material on the site was illegal. To make matters worse, the seizures were effectuated by ordering DNS registrars to reroute traffic away from these websites to servers operated by the Department of Justice, a technique that lead some to claim it would "break the Internet" when it was later contemplated in SOPA.[11]

The seizures were done using copyright's often-overlooked civil forfeiture statute.[12] Civil forfeiture statutes allow the government to seize property implicated in criminal activity without prosecuting anyone for a crime.[13] While copyright has long had a forfeiture provision, the 2008 PRO-IP Act radically expanded it to allow the government to seize essentially any property used in any manner to commit or facilitate criminal copyright infringement.[14] The law treats these seizures like any other contraband, ignoring the fact that nearly all seizures done in the name of copyright are seizures of speech, and the line between constitutionally protected speech and unlawful infringement is often quite uncertain.

Civil forfeiture is also an especially nefarious way to go about censoring speech, because reclaiming inappropriately seized property is a notoriously long and difficult process.[15] This is best illustrated by what happened next in Operation In Our Sites. Two of the websites—dajaz1.com, a popular hip-hop music blog, and rojadirecta.org, a website that aggregated links to streaming sports broadcasts—challenged the seizures and tried to get their domains released. In both cases the Department of Justice objected and held the domain names for more than a year before dismissing their cases and releasing the domains without any explanation.[16] No court ever determined whether the procedures used were unconstitutional, and the law is still on the books.[17]

A staggering array of proposals have come from the content industry to revisit SOPA, including a "notice and staydown" regime, use of the All Writs Act, or development of voluntary initiatives.[18] But a major part of what made SOPA so offensive does not need rebirth; it is already alive. The laws around Operation In Our Sites bear many of the same obvious First Amendment shortcomings.[19] And whether the same mobilization that stopped a law can be called upon to repeal an existing law remains to be seen.

Notes

1 The Stop Online Piracy Act, H.R. 3261, 112th Cong. (2011). Its Senate analogue, PIPA, was an acronym for the "PROTECT-IP Act," itself a backronym of the Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act, S. 968, 112th Cong. (2011). The first version was a Senate bill named COICA, the Combatting Online Infringement and Counterfeits Act, S. 3804, 111th Cong. (2010). For ease the essay refers only to the most famous of the trio of bills.

2 See Yochai Benkler et al., "Social Mobilization and the Networked Public Sphere: Mapping the SOPA-PIPA Debate," 2013, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2295953/; Jack Balkin, "Old School/New School Speech Regulation," 127 Harvard Law Review 2296, 2320 (2014).

3 See Letter from Laurence H. Tribe to Congress, December 6, 2011, http://www.scribd.com/doc/75153093/Tribe-Legis-Memo-on-SOPA-12-6-11-1; see also Letter from Marvin Ammori to Congress, December 8, 2011, http://ammori.files.wordpress.com/2011/12/ammori-first-amd-sopa-protectip.pdf (making similar arguments). Both of these were in response to an earlier letter written by noted First Amendment scholar Floyd Abrams, in favor of SOPA. See Letter from Floyd Abrams to Lamar Smith, November 7, 2011, http://www.sagaftra.org/files/sag/documents/SOPA_LetterbyFloyd%20Abrams11-7-11.pdf.

4 For the origin of the term, see Henry P. Monaghan, "First Amendment 'Due Process,'" 83 Harvard Law Review 518 (1970); see also Freedman v. Maryland, 380 U.S. 51, 58 (1964); Dawn Nunziato, "How (Not) to Censor: Procedural

First Amendment Values and Internet Censorship Worldwide," 42 Georgetown Journal of International Law 1123, 1128-29 (2011). Despite admonitions in other areas that courts should look at the effect of government action regardless of label, copyright-infringing speech has held a different place in free speech doctrine than other similarly situated speech, a subject that has been responsible for the deaths of many trees. See, e.g., Mark A. Lemley & Eugene Volokh, "Freedom of Speech and Injunctions in Intellectual Property Cases," 48 Duke Law Journal 147 (1998); Yochai Benkler, "Through the Looking Glass: Alice and the Constitutional Foundations of the Public Domain," 66 Law & Contemp. Problems 173 (2003); David Lange & Jefferson Powell, No Law: Intellectual Property in the Image of an Absolute First Amendment (2009). The techniques described here, however, go beyond even those already tolerated in copyright enforcement, and courts are beginning to recognize the importance of speech considerations in copyright more generally. See Salinger v. Colting, 607 F.3d 68 (2d Cir. 2010) (denying a preliminary injunction on free speech grounds).

5 For the canon of Supreme Court cases on this point, see Fort Wayne Books, Inc. v. Indiana, 489 U.S. 46 (1989); New York v. P.J. Video, Inc., 475 U.S. 868 (1986); Roaden v. Kentucky, 413 U.S. 496 (1973); Heller v. New York, 413 U.S. 483 (1973); Lee Art Theatre, Inc. v. Virginia, 392 U.S. 636 (1968) (per curiam); Freedman, 380 U.S. 51; Quantity of Books v. Kansas, 378 U.S. 205 (1964) (plurality opinion); Bantam Books v. Sullivan, 372 U.S. 58 (1963); Marcus v. Search Warrants, 367 U.S. 717 (1961); see also Alexander v. United States, 509 U.S. 544 (1993) (distinguishing between these cases and seizures done after a full trial on the merits).

6 Ctr. for Democracy & Tech. v. Pappert, 337 F. Supp. 2d 606, 658 (E.D. Pa. 2004). This is true, even though the standard for both – the "probable cause" standard – is the same. P.J. Video, 475 U.S. 868.

7 Just what judicial intervention was contemplated in SOPA is a bit of a mystery. The bill declared that "a court may issue a temporary restraining order, a preliminary injunction, or an injunction, in accordance with rule 65 of the Federal Rules of Civil Procedure … to cease and desist from undertaking any further activity as a foreign infringing site." Stop Online Piracy Act, supra note 1, at § 102(b)(5). It was never made clear what exactly the Attorney General must show for this, or what authority the court would have to scrutinize this, beyond the traditional theories of equitable powers and the additional limitations on temporary restraining orders found in the Federal Rules of Civil Procedure. See Fed. R. Civ. P. 65(b)(1); Jonathan Zittrain, Kendra Albert, and Alicia Solow-Niederman, "A Close Look at SOPA," The Future of the Internet, December 2, 2011, http://blogs.law.harvard.edu/futureoftheinternet/2011/12/02/reading-sopa/. This absence of articulated procedure would seem to go against the holdings of the cases noted in footnote 5, supra.

8 For a deep discussion of prior restraint and links to other resources, see Balkin, supra note 2, at 2315-16.

9 For a much longer piece I wrote about these seizures and their constitutionality, see Andrew Sellars, "Seized Sites: The In Rem Forfeiture of Copyright Infringing Domain Names," May 8, 2011, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1835604; see also Karen Kopel, "Operation Seizing Our Sites: How the Federal Government is Taking Domain Names Without Prior Notice," 28 Berkeley Technology Law Journal 859 (2013).

10 The sites involved included tvshack.net, movies-links.tv, zml.com, now-movies.com, thepiratecity.org, planetmovies.com, filespump.com, rapgodfathers.com, torrent-finder.com, rmx4u.com, dajaz1.com, onsmash.com, hq-streams.com, atdhe.net, firstrow.net, channelsurfing.net, ilemi.com, and rojadirecta.org. See Sellars, supra note 9, at 13.

11 Keith Dawson, "Gov't Crackdown Spurs Initiatives to Route Around DNS," IT World, December 7, 2010, http://www.itworld.com/legal/129947/net-censorship-dns-alternative; see "PROTECT IP / SOPA Breaks the Internet," Fight for the Future, https://www.fightforthefuture.org/pipa/.

12 18 U.S.C. § 2323.

13 Civil forfeiture was long a product of admiralty law, before seeing its expansion to organized crime and narcotics. Critics of the regime are numerous. See, e.g., Leonard W. Levy, A License to Steal: The Forfeiture of Property (1996).

14 18 U.S.C. § 2323(a)(1)(B). PRO-IP is yet another backronym, this time for the Prioritizing Resources and Organization for Intellectual Property Act of 2008, Pub. L. No. 110-403, 122 Stat. 4256 (2008). Prior to this law, copyright's civil forfeiture provisions only allowed for the seizure of infringing copies of works and the "plates, molds, masters, tapes, film negatives, or other articles by means of which" copies may be reproduced. 17 U.S.C. § 509(a) (repealed 2008).

15 See generally 18 U.S.C. § 983. These standards are actually a step more lenient than the prior civil forfeiture law, which previously completely shifted the burden of proof to the those seeking the release of property. See United States v. $80,180.00 in Currency, 303 F.3d 1182 (9th Cir. 2002). Under either standard, however, the initial seizure happens with only probable cause. § 981(b).

16 See Balkin, supra note 2, at 2319; In the Matter of the Seizure of the Internet Domain Name "DAJAZ1.COM", Elec. Frontier Found., https://www.eff.org/cases/matter-seizure-internet-domain-name-dajaz1com; Mike Masnick, "Oops: After Seizing & Censoring Rojadirecta for 18 Months, Feds Give Up & Drop Case," Techdirt, Auguse 29, 2012, https://www.techdirt.com/articles/20120829/12370820209/oops-after-seizing-censoring-rojadirecta-18-months-feds-give-up-drop-case.shtml. There appears to be only one court order from either case addressing any possible First Amendment issues with this, which determined that the website's 35% reduction in traffic after it reopened under another domain name and the closure of its discussion forums did not justify the domain name's release as a "substantial hardship." Puerto 80 Projects, S.L.U. v. United States, No. 11-cv-4139 (S.D.N.Y. Aug. 4, 2011). The court does not engage with Supreme Court precedent that appears directly contrary. See, e.g., Simon & Schuster, Inc. v. Members of N.Y. State Crime Victims Bd., 502 U.S. 105 (1991) (finding that indirect financial interference with speech based on its content is unconstitutional).

17 The law is still used with some regularity for the seizure of property connected with the sale of counterfeit goods. See,

e.g., United States v. 335 Counterfeit NFL Jerseys, No. 13-cv-341, 2014 WL 2575446 (E.D. Cal. June 9, 2014); United States v. Real Property and Premesis Located at 294-20 Cambria Avenue, No. 13-cv-6730, 2014 WL 2198618 (E.D.N.Y. May 27, 2014); United States v. $5,253 in Currency, No. 11-cv-6335, 2014 WL 122254 (W.D.N.Y. Jan. 13, 2014). In its bimonthly reports, the United States Intellectual Property Enforcement Coordinator reported several more iterations of "Operation In Our Sites," but all of them focused on websites selling counterfeit merchandise instead of allegedly infringing speech. See IPEC: Media and Spotlights, U.S. Intellectual Property Enforcement Coordinator, http://www.whitehouse.gov/omb/intellectualproperty/spotlight.

18 See Mike Masnick, "The Rebranding of SOPA: Now Called 'Notice and Staydown,'" Techdirt, March 14, 2014, https://www.techdirt.com/articles/20140313/17470826574/rebranding-sopa-now-called-notice-staydown.shtml (discussing "notice and staydown"); Russell Brandom, "Project Goliath: Inside Hollywood's Secret War Against Google," The Verge, December 12, 2014, http://www.theverge.com/2014/12/12/7382287/project-goliath (discussing the All Writs Act, 28 U.S.C. § 1651); A Call for Action for Online Piracy and Counterfeiting Legislation, ABA Section of Intellectual Property Law 90-91 (2014), http://www.americanbar.org/content/dam/aba/administrative/intellectual_property_law/advocacy/ABASectionWhitePaperACallForActionCompositetosize.authcheckdam.pdf (discussing a mix of remedies, including private efforts).

19 Balkin, supra note 2, at 2319.

ABC v. Aereo, Innovation, and the Cloud

Christopher T. Bavitz

The act of storing, accessing, or delivering content online can implicate the exclusive rights that Section 106 of the United States Copyright Act confers upon copyright owners. For some types of works (including audiovisual works), those exclusive rights include the right to perform or transmit those works to the public.

The US Supreme Court addressed the scope of the public performance right in a major decision this year, ABC v. Aereo, 134 S.Ct. 2498 (2014). Certain features of the case—including the unique nature of the service that Aereo offered—suggest that the Court's holding might be limited. But, the Aereo ruling has the potential to impact a wide range of services that grant users access to content stored in locations other than those users' own hard drives.

Aereo allowed each of its paid subscribers to rent one of thousands of small antennas that Aereo installed in a warehouse. Each antenna picked up over-the-air broadcast television signals and delivered programming via the Internet to the subscriber assigned to that antenna, at the subscriber's request. The service offered an alternative to cable or satellite for consumers who could not easily receive over-the-air broadcast signals and facilitated cord-cutting for those who wanted to watch network programs via the Internet.

Aereo argued that its service was effectively like an antenna that any viewer might connect to her TV set and use to access free broadcast signals; Aereo did not publicly perform the copyrighted programs that its subscribers accessed, and it thus did not infringe content owners' rights. Several TV producers and broadcasters claimed, to the contrary, that Aereo publicly performed their copyrighted television programs by transmitting them to viewers, much like cable providers that carry local broadcast stations. Cable providers pay to license broadcast programming; Aereo did not.

Those producers and broadcasters filed a federal lawsuit against Aereo claiming copyright infringement, and the Supreme Court ruled in favor of the plaintiff copyright owners. The Court's decision rested upon two major sets of discrete (and important) conclusions. First, the Court held that Aereo itself "performed" the works at issue, even though its subscribers selected whether and when to view content and which content to view. Second, those performances by Aereo were held to be performances or transmissions to the public, notwithstanding the fact that each antenna delivered content to only an individual Aereo subscriber.

The long-term legacy of the Aereo decision remains to be seen, but it offers some lessons for anyone seeking to innovate in a heavily-regulated environment and, in particular, those looking to develop cloud-based storage and content delivery systems.

On the broader innovation front, it is worth noting that the complex architecture of Aereo's system, with its thousands of tiny antennas assigned to thousands of individual subscribers, seemed driven at least as much by legal considerations as technical ones. Aereo launched in New York City, and a

prior decision from the federal appellate court that includes New York within its jurisdiction seemed to offer Aereo a roadmap for developing the one-antenna-one-subscriber model that was its hallmark.

In Cartoon Network, LP v. CSC Holdings, Inc., 536 F.3d 121 (2d Cir. 2008) (widely known as the "Cablevision" case), the United States Court of Appeals for the Second Circuit held that Cablevision's "Remote Storage DV-R" system did not infringe TV content owners' copyrights. The system allowed cable subscribers to record shows to and play them back from hard drives housed centrally in a Cablevision-operated facility (rather than on hard drives housed in set-top boxes in the subscribers' homes).[1] Each user of the system was assigned her own hard drive, and each user made her own decisions about which shows to record and whether and when to play them back. Content owners argued that Cablevision made unauthorized copies of their programs and engaged in unauthorized public performances or transmissions to subscribers. The Court disagreed, finding that Cablevision subscribers (not Cablevision itself) made the copies and that the transmissions of those shows to individual subscribers were not transmissions to the public.

The analogy between the service offered by Aereo and that offered by Cablevision has at least some surface appeal:

- An individual may lawfully connect a VCR or a set-top digital video recorder to her television at home, record shows, and watch them at a later date. And, Cablevision holds that she may do so even if the DVR is moved to a remote facility.
- An individual may lawfully connect an antenna to her television at home and watch programming delivered via over-the-air broadcast signals. The logic of Cablevision dictates that she may do so even if the antenna is moved to a remote facility.

Not only did the Supreme Court see the case differently, it did so in a decision that cited Cablevision only once in its eighteen pages of analysis.

The result in Aereo underscores the inherent volatility of innovating in a space governed by limited legal precedent, in reliance on modern interpretations of statutes drafted long before the technology at issue was contemplated (let alone invented). Critics of Aereo suggested that the service was taking advantage of a legal loophole; proponents reframed the service as simply following the law set forth by the Second Circuit's Cablevision decision. But, as the Court's ruling demonstrates, the law can be uncertain, especially as it concerns new technology.

On the specific legal questions at the heart of the Aereo decision, one cannot ignore the setting of the case. Aereo's position—that it was entitled to offer broadcast television programming to its users without paying fees to content owners—took direct aim at long-standing licensing regimes that permit cable providers to offer broadcast channels to their subscribers in exchange for royalty payments to the broadcasters. Although the Court's decision ostensibly turned on technical application and interpretation of language in the Copyright Act—including definition of the term "transmission" and analysis of what it means for a transmission to be "to the public"—the Court noted that the functions of Aereo (which paid no royalties) mirrored functions offered by cable companies (which paid royalties). The Court referred to "Aereo's overwhelming likeness" to cable companies, and Justice Scalia in

his dissent characterized the majority's decision as imposing "Guilt By Resemblance."[2]

It is difficult to say how the case would have come out if Aereo did exactly what it did as a technical matter but was not so blatantly and forcefully upending the existing business models and licensing regimes on which its competitors relied. But, the decision suggests that copyright law—which is ostensibly concerned with technicalities—may lend itself to more functional applications that look at the practical impact of a piece of technology rather than its narrow technical contours.

For what it's worth, the Supreme Court went out of its way in the Aereo decision to say that its holding was limited to the facts before it and expressly concluded by noting that questions about the implications of copyright law on other technologies—including cloud computing—should await cases "in which they are squarely presented."[3] Whether or not the specific holding of Aereo is limited, one can be certain that lower courts grappling with those other technologies will look to Aereo for guidance in the coming years.

Notes

1 It has long been established that a person recording television programs at home for purposes of "time shifting"—i.e., making a copy of a show now in order to watch it later, perhaps at a more convenient time—does not infringe copyright. See Sony Corp. of America v. Universal City Studios, Inc., 464 U.S. 417 (1984).

2 ABC, 134 S.Ct. at 2501, 2515.

3 Id. at 2511.

The Spanish Origins of the European "Right to be Forgotten": The Mario Costeja and Les Alfacs Cases

Ana Azurmendi

On 13th May 2013, the European Court of Justice recognised the right to be forgotten in the Mario Costeja case (2012), an action brought before this court for which another Spanish case, Les Alfacs (2010), had set a precedent.

Mario Costeja had suffered damages over the years as a result of an advertisement for a foreclosure sale, related to debts he owed to the Social Security administration, placed in the La Vanguardia newspaper in 1998. When the newspaper was digitalised, Google searches for the name Mario Costeja revealed personal data and financial information that are at present incorrect. This greatly affected his professional life. Costeja first filed a petition before the Spanish Data Protection Agency (SDPA) requesting that they require the newspaper to remove the information, yet his petition was not successful. The SDPA stated that the advertisement published in the La Vanguardia newspaper was legal, and that its removal would infringe freedom of expression. Nevertheless, the SDPA sent a request directed to Google Spain and Google Inc., calling upon these companies to stop indexing the aforementioned content. Google filed an appeal against the Agency's decision—and other similar decisions—before the National High Court. It was this judicial authority that ultimately referred this question for a preliminary ruling before the European Court of Justice.

As for the Les Alfacs case, it concerned a company that owned a campground. In 2010 the company filed a lawsuit against Google Spain for ignoring an earlier petition requesting that the search engine stop placing in its top results news about a horrific tragedy that took place on their campsite in 1978, when a truck transporting propylene exploded, leaving 243 dead. The complainants demanded both the right to be forgotten and the company's rights to honour, privacy, and self-image. The company wanted Google to filter the search results and differentiate between those who were looking for information on the tragedy and those who merely sought information about the campground, given that the way Google presented the search results at that time resulted in serious damages for the company.

In both cases, the personal information involved in the cases had been disseminated in proportion to its relevance when it was initially published. Nevertheless, the fact that this information was still widely available to a large audience ten to fifteen years after the original incidents did not appear to be logical if, on the one hand, it caused substantial moral and economic damages and, on the other, if the circumstances that led to its publication no longer existed. For this very reason, the right to be forgotten offers a solution that helps prevent longlasting damages while respecting freedom of expression (it is worth nothing that the ruling is controversial; experts disagree on the effectiveness of the approach[1)]. This could entail establishing a reasonable timeframe for universal access to this type of information, and afterwards either: a) removing the original identifying information from the source, substituting it for initials or, b) considering instituting a two-step barrier before being able to access the information. In the latter approach, after a reasonable timeframe, the original information would be transferred to a periodical archive that would only be accessible through the media source's website, and not directly through the search engines.[2]

Notes

1 See, for example, Jonathan Zittrain, "Troubling Solution to a Real Problem," *Internet Monitor 2014*, 33.

2 See, for example, the draft Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), October 22, 2013, http://www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf; and the opinion of Advocate General Jääskinen in Google Spain v. Agencia Española de Protección de Datos Mario Costeja, June 25, 2013, http://curia.europa.eu/juris/document/document.jsf?text&docid=138782&pageIndex=0&doclang=EN&mode=req&dir&occ=first&part=1&cid=362663.

Troubling Solution to a Real Problem

Jonathan Zittrain

This essay previously appeared in U.S. News & World Report.

2014 saw an extraordinary move by the European Court of Justice to compel search engines like Google and Bing to allow individuals to demand the removal of certain search results returned by their names.[1] Whether or not you support such a right in theory, the ECJ's chosen implementation raises several big problems.

First, should the search engine decide not to act upon the request, the person making the request can appeal—but there is no parallel mechanism for anyone else, such as the affected website, to appeal when the search engine grants a request. Moreover, when that happens, a removal appears to be permanent, even though changing circumstances might make an initial removal no longer warranted. For example, the requester might become a public figure, making previously irrelevant information vitally relevant. Or the contents of a webpage such as a Wikipedia entry might be changed to remove or amend the information in controversy. Or the requester could die, affecting his or her rights to the sorts of reputation shaping the ECJ contemplates. Affected sites should have a formal path to appeal search engine takedowns, and the grantings of takedown requests should be for a limited time, with an opportunity for the requester to re-lodge a request before expiration of a previous successful takedown.

Second, especially because the takedowns themselves are currently unreported to all but an affected website—and even that notification is, in some quarters, being challenged by authorities—there will be no way to analyze how the new right is being invoked and granted. There should be a means for academics willing to respect subjects' privacy to study takedowns, discern patterns, and report in aggregate how the right is evolving and what sorts of requests are being granted versus denied. We are likely to see more and more automated requests, with some people using specially developed intermediary reputation services that will perform rapid searches on the users' names, automatically categorizing results as negative, neutral, or positive, and then acting as the users' agents to file automatic takedown requests. This could result in a large volume of requests untouched by human hands, including those of the requester—likely not an outcome contemplated by the European court.

Finally, there is a puzzling triumphalism among some who view the ECJ's decision as a victory for European sovereignty. It's true that the decision compels Google, Microsoft, and others to consider EU law in rendering search results, and perhaps under European pressure, around the world rather than simply through European-branded versions of their products. But the core holding is a mandate for Google and others to hand-tweak results, breaching a longstanding editorial-style barrier that reputable search engines have taken pride in maintaining. For example, Google for many years has offered an explanation to those curious, and at times outraged, to find that a search on the word "Jew" often points to an anti-Semitic site as its first hit. That explanation—http://www.google.com/explanation.html—indicates an unwillingness by Google to hand-adjust search results to suit particular tastes, including its own. Rather, Google undertakes broad changes to its search algorithm in the name of increasing relevance or combatting spam and other search engine optimization. To ask Google and

others to adopt the habit of adjusting search results for very specific outcomes risks more broadly breaching the editorial barrier that has served as one of the public's best defenses against propaganda by centralized services like Google and Bing. It would be an irony if the very decision seen as re-asserting regulatory sovereignty over intermediaries instead unleashed far more self-conscious, but still secret, information shaping by them.

With luck, 2015 will see arrangements between the major search engines and academic institutions, especially European ones, to facilitate study of these phenomena, so that a right created to serve the public interest can be evaluated against it. Without these arrangements, I can only join others in having a hunch in how it's playing out—and mine is that the ECJ has come up with a bad solution to a very real problem.

Notes

1 Jonathan Zittrain, "The Ten Things that Define You," Future of the Internet, May 15, 2014, http://blogs.law.harvard.edu/futureoftheinternet/2014/05/15/the-ten-things-that-define-you/.

Community Mesh Networks: The Tradeoff Between Privacy, Openness, and Security

Primavera De Filippi

The Internet is weak, and this weakness has grown in recent years as the Internet has become more and more centralized, both at the application layer (with a concentration of power in the hands of a few large online operators) and at the infrastructure layer (governed in the United States by a few large telecom operators, such as Comcast, Verizon, and AT&T).

In face of the Snowden revelations, we are witnessing today a revived interest in mesh networking technologies promoting a more decentralized, peer-to-peer approach to network infrastructure and connectivity. Mesh networks are often reported as being more resilient and secure than the Internet, and it is not uncommon for people to regard them as a reactionary measure to the massive and generalized surveillance undertaken by the NSA. Their decentralized character is often regarded as a means to keep communication running during a period of crisis, while also providing a safe haven for activists eager to escape from both surveillance and censorship. This leads people to assume that mesh networks alone can resolve most of the privacy and security concerns of the Internet network—an assumption that is, unfortunately, often untrue.

Of course, mesh networks can be—and have been—made highly robust and secure, e.g., in the context of military-grade mesh networks deployed in war zones. Yet, these networks are extremely restricted in their use: they are configured to allow only a predetermined set of people to connect to them, and all communications are encrypted through proprietary algorithms that remain secret and internal to the network.

In the case of open community mesh networks, the situation is much different. Most of these networks are meant to provide an Internet connection to an underserved area with little or no telecommunication infrastructure and are designed to be as open and inclusive as possible: anyone can use the network or even connect a new node to the network.

In this regard, the decentralized and collaborative nature of community mesh networks might actually run counter to the security and privacy of users. To the extent that they are operated by the community, these networks also need to be secured by the community. Although many tech savvy users are involved in the initial set up of a mesh network, most of the users that subsequently connect to it are unlikely to spend much time securing the network. Hence, if a network is only as secure as its weakest node, most mesh networks deployed today are likely to be less secure than the vast majority of commercial ISPs.

Connectivity also constitutes an important challenge to the privacy and security of a network. While mesh networks make it easier to "route around damage," the need to acquire an uplink to the global Internet constitutes an important bottleneck. The interconnection point is exactly where the problem lies: once connected to the Internet, whether a user connects to an online operator (such as Google or Facebook) through a mesh network or a standard Internet connection doesn't make much difference

in terms of privacy or confidentiality: all data submitted to a third-party operator will effectively be controlled by it.

So far, the issue has only been addressed by a few community networks (e.g., FunkFeuer from Austria, NEDWirelles from Croatia, and WIan Slovenija) that have established a wireless backbone spanning geographical borders to create a direct link between them.

Today, as the technology is starting to be well understood, a growing number of mesh networks are being deployed all over the world. Mesh networks were initially difficult to deploy, as every node had to set up its own server and configure the routing protocol to use. Just a few years ago, the Commotion Wireless project (an initiative from the Open Technology Institute of the New America Foundation) was set up to address this problem by developing "Internet in a suitcase": an open source toolkit that can be readily installed on a variety of low-cost, off-the-shelf devices for anyone to set up a mesh network without any technical knowledge. Similar tools are also being developed by other communities (such as MeshNet, NodeWatcher, or the Serval Project in Australia); some even provide pre-installed and pre-configured hardware devices, such as the Open-Mesh routers from MIT that only need to be plugged in to provide mesh connectivity. A few months ago, Open Garden released FireChat, an end-user application allowing anyone with an iPhone or an iPad to create a modular mesh network by exploiting the Bluetooth connectivity provided by iOS 7. It only took a few weeks for a similar functionality to be enabled on Android phones, so that both iOS and Android users can now communicate on the same mesh network.

Perhaps, as more of such applications are deployed on standard end-user devices, we might soon witness the mainstream adoption of mesh networking technologies, and hopefully the revival of an open and decentralized Internet infrastructure respectful of the end-to-end principle and devoid of any bottlenecks or gatekeepers.

Warrant Canaries Beyond the First Amendment[1]

Jonathon W. Penney

Warrant canaries have emerged as an intriguing tool for Internet companies to provide some measure of transparency for users while also complying with national security laws, or so the argument goes.[2] How do they work? A warrant canary is a statement that an Internet company regularly publishes indicating it has not yet received a legal process that, if received, the company would be prohibited from disclosing.[3] Once such a legal process is received, the Internet company removes the statement, providing a kind of silent signal or warning.[4] Like the canaries in coal mines, the warrant canary is meant to warn users about the presence of a threat; here, it is not the presence of noxious gas, but overreaching government activities that may threaten rights.

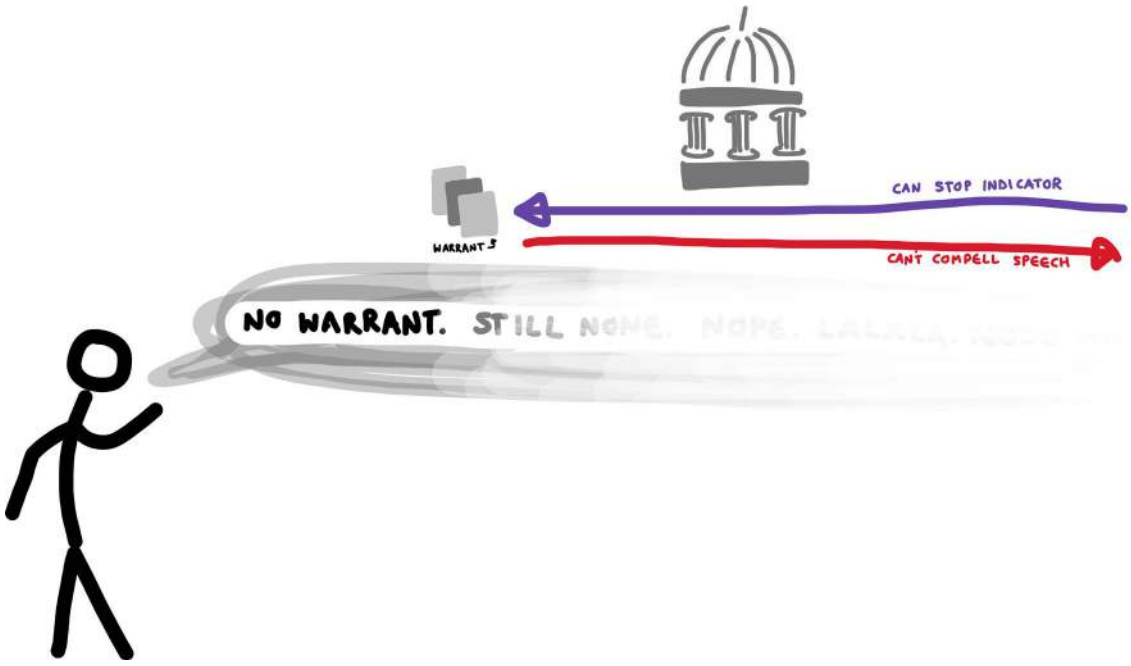


Illustration by Willow Brugh

Warrant canaries have been predominantly employed by Internet companies based in the United States—like Apple, Tumblr, Silent Circle, SpiderOak, and Pinterest—and typically appear in transparency reports about user data.[5] These American origins are not surprising, as warrant canaries are essentially designed for US law. While the US authorities may be able to "gag" or prevent Internet companies from talking about secretive legal processes they receive,[6] the theory is the First Amendment would prevent the government from compelling Internet companies from continuing to publish the warrant canary.[7] This is known as the First Amendment's "compelled speech" doctrine. Though there is very little scholarship on point and no cases testing the theory, there is at least a reasonable argument for the legality of warrant canaries in the US, as one recent analysis has concluded.[8] The

same cannot be said for the use of warrant canaries elsewhere. Why is this a problem? First, national security surveillance is today internationalized, particularly among close Western allies. The "Five Eyes" intelligence agency countries—the US, United Kingdom, Canada, New Zealand, and Australia—have a secret treaty that governs information sharing and surveillance cooperation as well as similarly secretive national security laws and processes.[9] There are also documented cases where these agencies have cooperated in order to flout domestic legal constraints on their surveillance activities.[10] Second, responding to similar transparency demands of users, Internet companies in these Five Eyes countries are now also considering employing warrant canaries.[11] Yet, despite the need, the legality of warrant canaries in any of these countries has yet to be explored. This comment aims to help fill that void—with an overview of warrant canaries' potential legality in the Five Eyes countries. Unfortunately, that legality is questionable at best.

Illustration by Willow Brugh

The warrant canary's legal theory assumes legal or constitutional restraints on compelled speech, that is, the power of the state to force a citizen to say something as opposed to merely restricting speech. The government could not, for example, compel Apple to publish a false statement that it had never received an order under Section 215 of the USA Patriot Act, if it had.[12] In Canada, law enforcement and national security agencies like the Royal Canadian Mounted Police (RCMP), Canadian Security Intelligence Service (CSIS), and Canadian is the Communications Security Establishment Canada (CSEC) all have the power to obtain "gag" or non-disclosure orders for legal processes served on Internet companies.[13] But what of compelled speech? Freedom of expression is protected under section 2(b) in the Canadian Charter of Rights and Freedoms, and the Supreme Court of Canada has recognized that this includes "the right not to say certain things"[14] or, as put by the Ontario Court of Appeal, the right "not to express certain views."[15] So, speech compelled by the government has been held to violate section 2(b) rights. But if a prima facie right violation is made out, the government can still argue, under section 1 of the Canadian Charter, that it is a reasonable limit—one that is "demonstrably justifiable in a free and democratic society."[16] This is likely a problem for warrant canaries, as Canadian courts have proven quite deferential to government justifications for compelled speech, finding it a reasonable limit on section 2(b) rights in a range of contexts, including a compelled oaths,[17] union fees,[18] tobacco health warnings,[19] as well as an order forcing an employer to "say" only certain objective facts in a statement while restricting any speech that contradicted those facts.[20] Courts would likely find national security or "anti-terrorism" objectives compelling or pressing reasons to justify such limits. In Canada, there is some legal potential for warrant canaries, but it is shaky at best.

Warrant canaries in New Zealand and Australia, two other Five Eyes countries, would face similar problems. In New Zealand, though the case law is not determinative, free speech protections under section 14 of the New Zealand Bill of Rights Act likely include a right "not to be compelled to say certain things."[21] However, the New Zealand Bill of Rights Act also contains a "justification" provision (section 5) worded exactly like Canada's, where limits on rights are constitutional if "demonstrably justified in a free and democratic society." New Zealand courts also apply a legal test for this section drawn from Canadian case law—the same legal test that led to deferential results on compelled speech in Canada.[22] With little case law on point, it is very difficult to determine the legality of warrant canaries; at the very least, it would be a highly risky move for a New Zealand Internet company to attempt at this point. The situation in Australia is more certain—warrant canaries have little legal basis. There is no explicit or implied constitutional protection for freedom of expression, nor right against compelled speech, in the country, beyond narrow common law limits. The Australia High Court, as recently as 2012, issued a landmark decision on compelled speech, finding that a law imposing sweeping forms of compelled speech on private companies—in the form of government prescribed standard packaging and intrusive health warnings for tobacco products—entirely constitutional.[23] Notwithstanding the broad scope of the government compelled speech, this result was, in light of scant Australian constitutional protections for this type of speech, in little doubt from the beginning.[24]

Finally, law in the United Kingdom likewise offers little comfort for warrant canary and transparency advocates. Public authorities in the UK such as the Government Communications Headquarters (GCHQ) can serve secret legal processes with non-disclosure orders under the Regulation of Investigatory Powers Act (RIPA). Law enforcement can also compel Internet companies to produce encryption keys under Part III of RIPA, itself a form of compelled speech. Interestingly, a practice of "tipping off"—comparable to warrant canaries—has been used in relation to such key disclosures. Here, parties state that if they voluntarily revoke a key, they will always explain why; but if they are secretly required to "revoke" by public authorities, they will offer no explanation, tipping off others.[25] Neither these "tipping off" practices nor warrant canaries have been legally tested, however, and the law offers few protections. The UK Human Rights Act (1998) includes rights to freedom of expression under Article 10, but this right is explicitly "qualified" and can be limited for a host of state objectives, including "national security," "territorial integrity," "public safety,, and "prevention of disorder," to name a few. These are the very objectives public authorities would likely cite to justify compelled speech in a national security investigation; they would also have explicit language to rely on for these limits in Article 10(2). What is more, "unwritten" common law speech protections are just as unhelpful.[26] Again, no clear legal basis exists for warrant canaries.

Internet companies today find themselves caught between growing user demands for transparency and government requirements that any secret national security requests made to those companies remain exactly that—secret. In this increasingly complex legal and regulatory space, warrant canaries offer a potentially innovative tool for greater transparency, but they may be, as Jonathan Zittrain has suggested, too clever by half.[27] Among the other countries in the Five Eyes intelligence alliance—all beyond the reach of broad US First Amendment protections—the legality of warrant canaries is murky and fraught with uncertainty; a risky venture for any Internet company to undertake.

Notes

1 This essay is based on a forthcoming legal article comparatively analyzing "compelled speech" and warrant canaries in the "Five Eyes" countries beyond the US.
2 Warrant canaries first appeared with respect to FBI requests of libraries: Jessamyn West, "The FBI, and Whether They've Been Here or Not," Librarian.net, September 9, 2013, http://www.librarian.net/stax/4182/the-fbi-and-whether-theyve-been-here-or-not/; Ben Johnson, "A Canary in the Coal Mine... and In Your Mac," Marketplace Tech, May 13, 2014, http://www.marketplace.org/topics/tech/canary-coal-mine-and-your-mac.
3 Kurt Opsahl, "Warrant Canary Frequently Asked Questions," Electronic Frontier Foundation: Deep Links, April 10, 2014, https://www.eff.org/deeplinks/2014/04/warrant-canary-faq.
4 Ibid.
5 Ibid.
6 Secret subpoenas under the Electronic Communications Privacy Act; Section 215 orders for bulk data under the Patriot Act; and Section 702 orders under the FISA Amendment Act, are part of this regulatory regime; legal processes that Internet companies receive accompanied by a "gag" or non-disclosure order. See Brennan Center for Justice, "FACT SHEET: Are They Allowed to Do That? A Breakdown of Selected Government Surveillance Programs," New York University School of Law, http://www.brennancenter.org/sites/default/files/analysis/Government%20Surveillance%20Factsheet.pdf.
7 Opsahl, ibid.
8 See Naomi Gilens, "Note: The NSA Has Not Been Here – Warrant Canaries as Tools for Transparency in the Wake of the Snowden Disclosures," SSRN, April 2014, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2498150.
9 Owen Bowcott, "'Five Eyes' surveillance pact should be published, Strasbourg court told," The Guardian, September 9, 2014, http://www.theguardian.com/world/2014/sep/09/five-eyes-surveillance-pact-appeal-disclosure-human-rights.
10 Colin Perkel, "Canadian spy agency withheld information from court to get warrants, judge says," The Toronto Star, December 20, 2013, http://www.thestar.com/news/canada/2013/12/20/canadian_spy_agency_withheld_information_from_court_to_get_warrants_judge_says.html; Ewen MacAskill, et al., "Revealed: Australian spy agency offered to share data about ordinary citizens," The Guardian, December 2, 2013, http://www.theguardian.com/world/2013/dec/02/revealed-australian-spy-agency-offered-to-share-data-about-ordinary-citizens; Glenn Greenwald, et al., "NSA shares raw intelligence including Americans' data with Israel," The Guardian, September 11, 2013, http://www.theguardian.com/world/2013/sep/11/nsa-americans-personal-data-israel-documents.
11 Alec Muffett, "TIL: What a Warrant Canary Is...," Dropsafe Blog, June 30, 2013, http://dropsafe.crypticide.com/article/11532; Doctorow, ibid (suggesting warrant canaries for the UK).
12 This is not an abstract thought experiment. See Iain Thomson, "Apple's Warrant Canary Riddle: Cock-Up, Conspiracy, or Anti-Google Point Scoring," The Register, September 20, 2014, http://www.theregister.co.uk/2014/09/20/apples_warrant_canary_is_either_cockup_conspiracy_or_the_antigoogle_selling_point/.
13 See Steven Penney, "National Security Surveillance in an Age of Terror: Statutory Powers and Charter Limits," Osgoode Hall Law Journal 247 (2010), 48.
14 Slaight Communications Inc. v Davidson, 1989 CanLII 92 (SCC), [1989] 1 SCR 1038 (Per Justice Lamar at para 95).
15 Rosen v Ontario (A.G.) (1996), 1996 CanLII 443 (ON CA), 131 DLR (4th) 708, at para 16 (Ont CA).
16 Section 1, Canadian Charter of Rights and Freedoms.
17 McAteer et al. v. Attorney General of Canada, 2013 ONSC 5895 (CanLII), http://canlii.ca/t/g0n32.
18 Lavigne v. Ontario Public Services Employees Union et al. (1991), 1991 CanLII 68 (SCC), 81 D.L.R. (4th) 545 (S.C.C.).
19 RJR McDonald Inc. v Canada (Attorney General), 1995 CanLII 64 (SCC), [1995] 3 SCR 199
20 Slaight Communications Inc. v Davidson, 1989 CanLII 92 (SCC), [1989] 1 SCR 1038.
21 As noted by one former Attorney General: Report of the Attorney General under the New Zealand Bill of Rights Act 1990 on the Sale of Liquor (Health Warnings) Amendment Bill.
22 Ibid at 2.
23 JT International v Commonwealth of Australia et al [2012] HCA 43. ABC News, "High Court rejects plain package challenge," August 15, 2012, http://www.abc.net.au/news/2012-08-15/high-court-rules-in-favour-of--plain-packaging-laws/4199768.
24 Melinda Upton and Jessie Buchan, "Australia: Australian High Court Rejects Challenge By Big Tobacco And Determines Plain Packaging Laws Are Constitutional And Valid," Mondaq, November 17, 2012, http://www.mondaq.com/australia/x/206502/Constitutional+Administrative+Law/tobacco+plain+packaging.
25 Foundation for Information Policy Research, "Key Revocation, Government Access to Keys and Tipping Off," FIPR Web, http://www.fipr.org/rip/BG_revoke.htm.
26 Cory Doctorow, "How to foil NSA sabotage: use a dead man's switch," The Guardian, September 9, 2013, http://www.theguardian.com/technology/2013/sep/09/nsa-sabotage-dead-mans-switch (noting the UK "unwritten constitution" to be unclear on point).
27 As quoted in: Ben Johnson, "A Canary in the Coal Mine... and In Your Mac," Marketplace Tech, May 13, 2014, http://www.marketplace.org/topics/tech/canary-coal-mine-and-your-mac.

Net Neutrality and Intermediary Liability in Argentina

Eduardo Bertoni[1]

Should all data be treated equally? Are communications platforms liable for their users' online activities? These two questions are at the heart of the current debates unfolding in Argentina related to net neutrality and intermediary liability, and their resolution will have far-reaching implications for user rights.

Many consider net neutrality to be guaranteed under Argentina's current web standards, specifically Decree 764/2000 establishing non-discrimination among service providers and Resolution 05/2013, which dictates that service providers may not arbitrarily interfere in users' access to online content. Others believe these standards could go further: the Center for Studies on Freedom of Expression and Access to Information (CELE) has been advocating for a legal reform that would unequivocally guarantee net neutrality and the associated rights to unhindered digital access. Over the past year, the Senate's Commission on Systems, Media, and Liberty of Expression has been working on draft legislation related to net neutrality and Internet rights, to which CELE and other members of civil society have been contributing. The Commission has taken the important step of soliciting feedback from diverse sectors that would be affected by the law under discussion, but the latest version nevertheless includes components that would undermine its stated commitment to neutrality.

For example, the draft proposes that the principle of neutrality apply only to "legal" content, applications, and services. Such a proposal implies a tricky negotiation of legality in terms of both scope and substance, and leaves unresolved which stakeholders would have the authority to establish the parameters of legality. Without clear guidelines on responsibility for determining legality, private sector companies that offer online services could have considerable leeway to block or filter content. Bestowing private sector companies, such as Internet service providers, with the power to censor content on the grounds of its legality risks impeding the exercise of fundamental information rights.

The draft bill also submits that certain "special services"—as yet unspecified—would be exempt from the principle of neutrality. The ongoing debates on net neutrality underway in the United States, the European Union, and elsewhere have underscored the complexity of the concept of "special services" and affirm that its inclusion in any legislative measure merits an in-depth discussion. The main recurrent problem related to special services is that there is not yet an agreed-upon definition of which services fall under this designation.

Lawmakers have also been mulling over legislative projects related to intermediary liability, which is not currently regulated in Argentina. This means that in rulings involving an intermediary—an Internet service provider, search engine, or platform—judges may invoke whatever norms they deem applicable to the case when considering whether or not the intermediary is accountable for the content. The complexity of intermediary liability has been put on display in Argentina in cases of high-profile public figures seeking the removal of undesirable online content; recently an Argentine model sued Google and Yahoo in "Rodríguez, María Belén c/ Google Inc s/ daños y perjuicios" for damages after pictures of her were linked to websites with sexual content. This case is pending before the Argentinean Su-

preme Court. In this and other cases under review, courts are charged with determining the responsibility of information gatekeepers such as these search engines. Given the specificity and range of cases that directly implicate the issue of intermediary liability, there is an urgent need for Argentina to legislate this issue without imperiling free expression.

The discussions surrounding net neutrality and intermediary liability signal that we, as users of Internet-based platforms and applications, are in the midst of a moment that may mark a fundamental shift in our technological lives. In Argentina, there is still time to avoid enacting into law errors that would privilege a small few at the expense of many.

Notes

1 Sophia Sadinsky, Princeton in Latin America Fellow at the Center for Studies on Freedom of Expression and Access to Information (CELE), contributed to this report.

Sexting, Minors, and US Legislation: When Laws Intended to Protect Have Unintended Consequences

Monica Bulger

In a terrible stroke of bad luck, 19-year-old Scott Lienhart was caught producing marijuana concentrate when police entered his backyard in pursuit of his roommate, who was attempting to outrun a minor in possession of alcohol charge. While searching the residence, sheriff detectives found what was described in their press release as 'child pornography' on Lienhart's cell phone, leading to Lienhart being booked on child pornography charges in addition to drug charges.[1] Yet how many 19-year-olds, very recently minors themselves, might have similar content on their phones? How do existing child pornography laws address sexting, in which minors produce sexually explicit images of themselves to share with other minors?

Existing US law prohibits the production, possession, sale, and distribution of child pornography, defined by Section 2256 of Title 18, United States Code as "any visual depiction of sexually explicit conduct involving someone under 18 years of age."[2] Penalties under child pornography laws can include fines, imprisonment, and registry as a sex offender. What is unclear in practice, however, is distinguishing between child sexual abuse images—in which the image is taken and distributed without consent or through violence or coercion, and which seem to be the intended target of existing law—and self-generated images taken by minors and willingly shared with other minors. Given the legislative grey area surrounding sexting, teens are potentially at risk of criminal charges for what has become a widespread practice.[3]

The relevance and applicability of laws intended to protect minors from the production of child sexual abuse images need further investigation in light of new practices of image sharing among teens. As incidents of arrests and criminalization of minors have been reported, Wolak, Finkelhor, and Mitchell (2012) urge a separation of "experimental" (cases involving only youth, with no abusive elements) from "aggravated" cases (in which an adult is involved, or a minor engaged in malicious, non-consensual, or abusive behaviour). In their review of 3477 cases of youth-produced sexual materials in 2008-2009, Wolak, et al. find arrests occurred in 18% of cases related to experimental behaviour, 36% of youth-led aggravated cases, and 62% of cases involving an adult. 63% of the images were distributed by cell phone and were not posted on the Internet. Sex offender registration only occurred in unusual cases.[4,5]

Returning to the case of Scott Lienhart, what remains unclear is the nature of the images. At what age did he receive them? What are the legal implications of keeping photos received as a minor, shared by minors, when one is no longer a minor? Wolak, et al. (2012) found that the majority of teen sexting images are consensually self-generated and not widely shared on the Internet. With the exception of the age of the participants, the conditions under which these images are created and distributed concretely differ from the abusive situations that existing child pornography laws address. Consideration of Wolak, et al.'s recommendations to apply "experimental" versus "aggravated" criteria to these cases might provide the nuance necessary to reduce vulnerabilities present under current legislation.

Notes

1 "UCSB student arrested for possession of child porn on his cell phone," press release from Santa Barbara Sheriff Office, January 14, 2014, http://www.sbsheriff.org/01151401.html.

2 Child exploitation and obscenity section, US Department of Justice, http://www.justice.gov/criminal/ceos/citizensguide/citizensguide_porn.html.

3 Hanna Rosin, "Why Kids Sext." The Atlantic, October 14, 2014, http://www.theatlantic.com/magazine/archive/2014/11/why-kids-sext/380798/.

4 J. Wolak, D. Finkelhor, and K. Mitchell, "How often are teens arrested for sexting? Data from a national sample of police cases," Pediatrics, 129, 1-8, 2012, http://pediatrics.aappublications.org/content/early/2011/11/30/peds.2011-2242.abstract.

5 Leonard Lopate, "Why do kids sext and is it a crime?" [Radio interview with Hanna Rosin and Marsha Levick], WYNC, October 24, 2014, http://www.wnyc.org/story/why-do-kids-sext-and-it-crime/.

Devices, Design, and Digital News for India's Next Billion Internet Users

Hasit Shah

India's IT industry is globally renowned, and the country has a well-deserved reputation for exporting top technical talent to the developed world. But in India, Internet penetration has been very low.

Until recently it hovered at around 10-15%,[1] leaving around a billion Indians without access, inevitably those with lower levels of education and smaller incomes (in other words, the ones who'd benefit the most from the information and opportunities available on the Internet).

But consider India's problems. Some might argue that there are bigger issues than a lack of broadband. Three hundred million people don't have electricity,[2] and a similar number are illiterate.[3] Half the population doesn't even have a toilet at home.[4]

The arrival of cheap cell phones has already had a dramatic impact on India. Its landline network was pretty useless for a lot of people: expensive, bureaucratic, cumbersome, and unreliable. Now everyone's got a mobile, including those without a regular power supply, those who can't read, and even the ones without a toilet. None of that is a prerequisite for owning and using a cell phone.

Now, smartphones are within touching distance of mass affordability. Where wired Internet still does not exist, i.e., in most of India, mobile networks are filling the gap. According to recent estimates, there will be around 350 million smartphone users in India by the end of 2014.[5]

But at the moment, not all of these low-end smartphones are connected to the Internet because a lot of the available content and platforms are simply not designed for the people buying the devices. Many people don't yet have a compelling enough reason to fork out the extra rupees.

Any mobile strategy in India must therefore take a two-pronged approach: in the short term, a platform must be light and simple enough to work on India's current smartphones and networks, while developers simultaneously prepare for the inevitable modernization of India's digital infrastructure in the longer term.

I spent a year as a Nieman-Berkman Fellow in Journalism Innovation at Harvard, trying to understand how news will fit into this enormous new digital ecosystem.

The most successful content and platforms in India, like anywhere else, demonstrate a deep understanding of their audiences. These are the key design challenges:

Language – Fewer than 10% of Indians are fluent in English,[6] so these new mobile Internet users are instead likely to communicate in one of India's 22 major languages (or more accurately, in one of countless dialects).

Literacy – 25% of the country is illiterate,[7] so we have to be careful about text. But many people still use these devices for music and photos. Digital literacy is an additional challenge.

Low-end tech – These are not iPhones on 4G. They mostly run on old versions of Android.[8] Videos often fail to load, and the connection itself can be erratic.

Low attention span – Smartphone users spend far more time on social media, entertainment and practical necessities like mobile money, than on news. We will need to figure out a way to make news engaging, necessary, and shareable.

Since most Indian users seem unlikely to go directly to news sites, we will need to go to the platforms they use most. The immediate future—and greatest opportunity—is with chat apps like Whatsapp (50 million users) and WeChat.[9] These are proper social networks that work well on low-end devices.

Media companies will address the challenges I've outlined above in different ways. The successful ones are likely to be those who can work out how to respond to users and build the right platforms, designed specially for this new, enormous, diverse audience.

Notes

1 Internet Monitor, "Access in India," http://thenetmonitor.org/countries/ind/access#.
2 "Access to electricity (% of population)," The World Bank, http://data.worldbank.org/indicator/EG.ELC.ACCS.ZS.
3 Internet Monitor, "Access in India," http://thenetmonitor.org/countries/ind/access#.
4 "India census: Half of homes have phones but no toilets," BBC, March 14, 2012, http://www.bbc.com/news/world-asia-india-17362837.
5 Charles Arthur, "Smartphone explosion in 2014 will see ownership in India pass US," The Guardian, January 13, 2014, http://www.theguardian.com/technology/2014/jan/13/smartphone-explosion-2014-india-us-china-firefoxos-android.
6 "Education," in Human Development in India: Challenges for a Society in Transition (Oxford: Oxford University Press, 2010), http://ihds.umd.edu/IHDS_files/06HDinIndia.pdf.
7 Internet Monitor, "Access in India," http://thenetmonitor.org/countries/ind/access#.
8 "Digital Statistics 2014—India," IdeateLabs, February 10, 2014, http://www.slideshare.net/iibea/digital-statistics-2014-india.
9 Trushar Barot, "How BBC News covered Indian elections on WhatsApp and WeChat," BBC, July 22, 2014, http://www.bbc.co.uk/blogs/blogcollegeofjournalism/posts/How-BBC-News-covered-Indian-elections-on-WhatsApp-and-WeChat.

Dispute Resolution in the Sharing Economy

Ethan Katsh and Orna Rabinovich-Einy

The Sharing Economy is often described in highly positive terms, referring to such values as sharing, collaboration, responsibility, trust, cooperation, and accountability.[1] In the aftermath of the economic downturn, such values were embraced and celebrated. New technologies, mainly the spread of social media and increased availability of smart phones, have fed into these developments and reinforced them. Law is often viewed as an intruder to this newly emerging paradise of sorts.[2]

Sharing-based endeavors, however, are no paradise. In almost any environment in which human beings interact and exchange goods and services, some misunderstandings, grievances, and conflicts occur.[3] While the Sharing Economy has received much attention, there has been limited thought devoted to the different types of conflict that arise in this environment and the ways in which they could be dealt with through emerging online dispute resolution ("ODR") tools and systems. Web 2.0 companies such as eBay created new marketplaces of goods that enabled anyone to sell anything to anyone else. Sharing Economy companies, such as Airbnb, Uber, TaskRabbit, RelayRides, and others,[4] are largely selling services, thus allowing anyone to sell any service to anyone else. In so doing, the Sharing Economy is creating and encouraging participation in many marketplaces, generating more varied and complex disputes among users, and requiring a rethinking of regulatory approaches in different industries.

When online auction sites were first established, they needed to persuade regulators that they were actually not in the auction business. This sleight of hand was largely successful, and online "auction" sites could proceed without being subject to the regulations that applied to offline auctions.[5] Sharing economy companies, by selling almost any kind of service, are in competition with a much broader range of businesses and have already been targeted by regulators in ways that eBay never experienced. It is not yet clear what the end result of this will be, and the experience of the earlier online goods marketplace does not seem to provide clear lessons. We are still in the early stage of the development of the Sharing Economy, with many ventures and experiments but little indication which will survive and thrive. Regardless of how the regulatory issues are resolved, however, systems will need to be put in place to handle disputes between those offering and those receiving services. Ebay was in business for four years before it recognized that it needed to provide an accessible online dispute resolution service.[6] While it previously had a feedback system in place that undoubtedly prevented conflict and influenced the willingness of buyers to participate in the marketplace, eBay eventually decided that an online dispute resolution process was also necessary. Currently, this system handles over 60 million disputes a year, essentially making it the largest small claims court in the world.

Disputes are a topic that most start-ups would prefer to ignore. Any new company's primary goal is to scale revenue, and dispute resolution is often viewed as a distraction or an investment of funds that are needed elsewhere. Advertising the existence of a dispute resolution process also acknowledges that disputes occur, something, we have often been told, entrepreneurs think can be hidden or at least not advertised. Lastly, these companies, borrowing from earlier models, often assume that

reputation and feedback systems are sufficient to deter bad actors.

Over time, eBay and others learned something that Sharing Economy companies will also need to understand. This is that disputes can actually be beneficial to a company. There are several reasons for this. The most obvious one is that dispute resolution represents a promise to users and potential users that if something goes wrong, it will be fixed. It helps build trust and reduces risk, thus influencing a user's willingness to try the system. In addition, and perhaps more importantly from the company's point of view, dispute resolution is important in identifying bad experiences. Ebay's former director of online dispute resolution has explained the value of responding to bad experiences as follows:

> As an example, imagine you were buying gifts for your family and friends over several weeks leading up to the holiday season… imagine that one of the items arrives and there is a problem. Maybe it was damaged in shipping, or maybe the wrong item was delivered. When that happens, you as the purchaser must pay individual attention to that particular transaction. You go back to your e-mail, search for the item receipt, and determine which marketplace the item was purchased from. Then you go to the website of the marketplace and try to determine what you need to do to get the problem resolved. That is the moment at which the buyer experiences an in-depth and unexpected interaction with an e-commerce market-place. That is the moment where loyalty is imprinted. If the marketplace provides an easy to find process for resolving the problem, a strong impression is made in the mind of the buyer. If the marketplace does not provide any easy to discover process for resolving the problem, the buyer's experience instead is one of frustration, which creates a strong impression in the other direction.[7]

Given the speed of communication online, bad experiences not only need to be addressed but addressed quickly. In an age of fast communication, social media, and online reputation sites, disputes cannot be hidden and, as a former customer service manager at TaskRabbit recently told us, "dispute resolution is the one thing that you can't get wrong."[8] Getting dispute resolution "right" in the sharing economy requires developing dispute resolution and prevention systems that fit the nature of the online environment. While the literature on dispute systems design recognizes the need to tailor dispute systems to the nature of disputes, parties and the setting in which they arise, they have often overlooked the role of technology in such systems. The sharing economy thus provides a fascinating case study for examining the characteristics of disputes in the internet age, the limitations of traditional avenues, and the potential of ODR mechanisms for addressing such disputes. It also provides an insightful arena for studying the evolution of new systems for addressing disputes in the digital age and the barriers that stand in the way of such development.

Notes

1 Sarah Horowitz, "Occupy Big Business: The Sharing Economy's Quiet Revolution," The Atlantic, December 6, 2011 http://www.theatlantic.com/business/archive/2011/12/occupy-big-business-the-sharing-economys-quiet-revolution/249582/ ("This sharing economy is based on people coming together to create their own markets (Airbnb), their own products (Etsy), and their own currency (TimeBanks). It relies on shared needs, trust and the belief that the groups is stronger than the individual."); see also Russ Roberts, "Blecharczyk on Airbnb and the Sharing Economy," EconTalk Episode with Nathan Blecharczyk, September 1, 2014, http://www.econtalk.org/archives/2014/09/nathan_

blecharc.html (Statement by Nathan Blecharczyk, co-founder and chief technology officer of Airbnb: "This whole marketplace is based on trust.").

2 Tom Slee, "Caring and Sharing," Jacobin, January 24, 2014, https://www.jacobinmag.com/2014/01/sharing-and-caring (Statement by Airbnb CEO Brian Chesky: "Cities can't screen as well as technologies can screen.").

3 See Tricia Duryee, "Airbnb's Rental Nightmare Ends in Arrest and One Still Very Unlucky Customer," AllThings, July 29, 2011, http://allthingsd.com/20110729/airbnbs-rental-nightmare-ends-in-arrest-and-one-still-very-unlucky-renter/ for a well-known Airbnb problem; for examples of TaskRabbit disputes, see https://news.ycombinator.com/item?id=4522475.

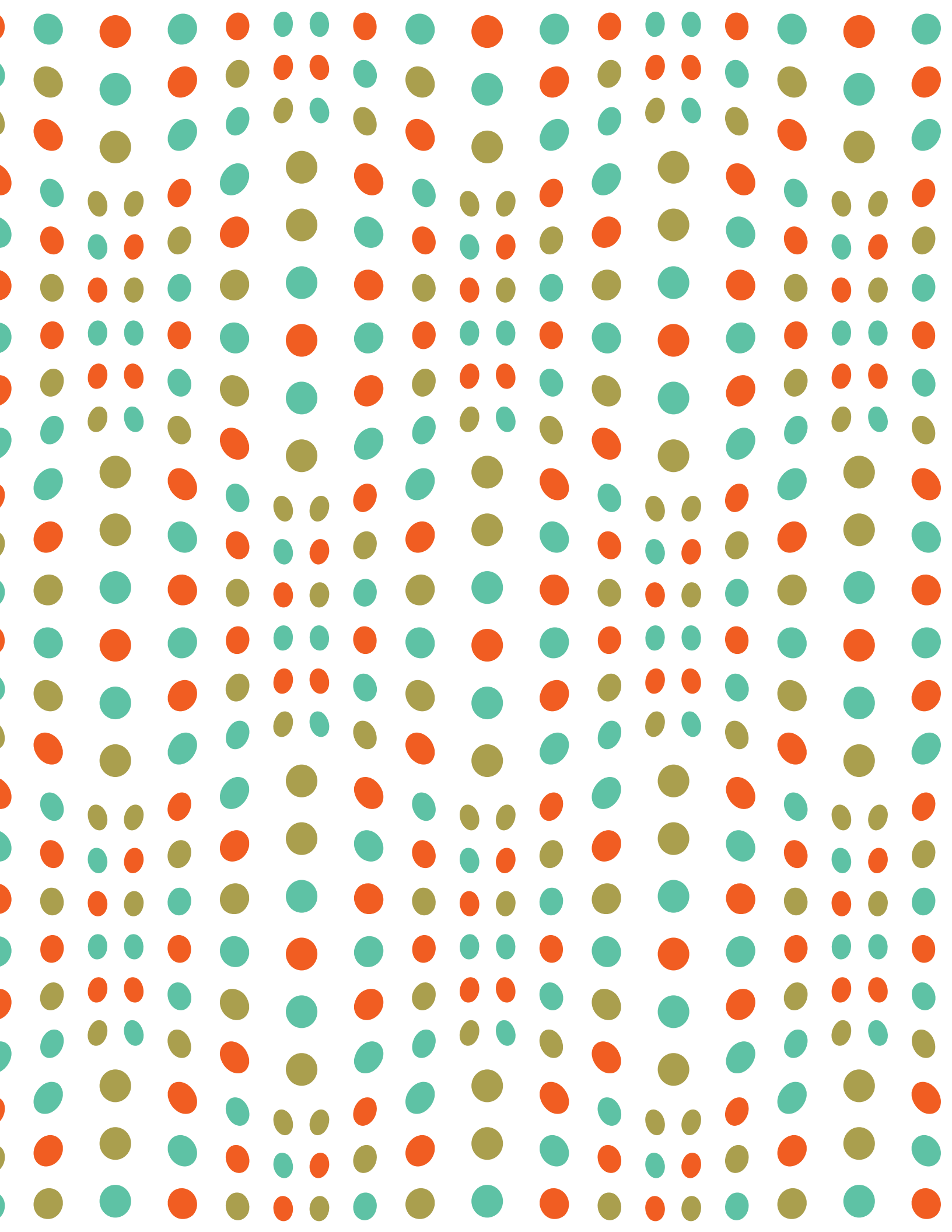
4 Other examples are Lyft, Snapgoods, DogVacay, Liquid, Poshmark, Fitmob, HomeJoy, MyWays, and Amazon Mechanical Turk.

5 "eBay is NOT an auction site," Simple Solutions, February 24, 2012, http://www.simplex-solutions.net/ebay-is-not-an-auction-site/.

6 E. Katsh, J. Rifkin, and A. Gaitenby, "E-Commerce, E-Disputes, and E-Dispute Resolution: In the Shadow of 'eBay Law,'" 15 Ohio St. J. on Disp. Resol. 705 (2000).

7 Colin Rule, "Quantifying the Economic Benefits of Effective Redress: Large E-Commerce Data Sets and the Cost-Benefit Case for Investing in Dispute Resolution," 34 U. Ark. Little Rock L. Rev. 767, 775 (2012).

8 Conversation with Nicolas Waldman, former Director of Trust and Safety at TaskRabbit, September 15, 2014.



DATA AND PRIVACY

Robert Faris and David R. O'Brien

The mismatch between traditional mechanisms for preserving privacy and the realities of digital networks are more apparent each day. The Internet, "the world's biggest copy machine,"[1] has eliminated the principal mechanism for preserving privacy; it used to be expensive to record and maintain information on the everyday comings and goings of citizens. Now that so many citizens travel with location tracking devices, volunteer to help fill out a digital map of their social networks—if not already fully captured by their phone records—and conduct their lives and share their thoughts in a machine readable format, the boundaries of privacy are harder than ever to define and protect.

Traditional privacy protection was premised on the notion of informed consent, that individuals would understand the implications of their choices to share personal information before making decisions to allow others to collect information on them. In any practical sense, this notion is obsolete in the digital age where users of Internet services habitually agree to lengthy "click-through" agreements without reading them. Privacy laws still rely heavily on this fictional premise that individuals are well informed about the terms under which they share data prior to giving consent.

Most studies on the subject indicate that we have a fuzzy understanding of what privacy means at best, and that our actions contradict our stated preferences on privacy; when asked in surveys, Internet users express growing concerns over online privacy, yet they continue to share a stunning amount of sensitive information online. The contradictions almost make sense if what we want is the right to control where, how, and with whom we share data, and if that principle is applied to a digital world in which the context is changing in ways we are not able to observe. In any case, the platforms and technologies that collect data about us are not designed to recognize and respect these subtle distinctions in context.

The potential benefits of mining big data for social good are legion. Improving the provision of health services, education, energy, and security is critically tied to better monitoring outcomes made possible through data collection and analysis.[2] There is a sizeable and hard-to-quantify overlap between eroding personal privacy and improving the provision and delivery of welfare enhancing goods. The future of both depends in part on the ability to reconcile these two. In the best of all worlds, we'll discover mechanisms to manage data flows that reveal this to be a false choice, such that privacy can be protected while using data for good. The alternative, and more likely, scenarios are defined by trade-offs and will require mechanisms to mitigate the most deleterious impacts of diminished privacy and additional protections to avoid the most egregious disclosures of private data.

Consumer privacy is inextricably tied up with issues of online security and government surveillance—the same architectures that allow private companies to collect personal data or encourage us to share this data also offer openings for third parties to access this same data, some of which is voluntary (e.g. the sale of data to advertisers), some compulsory (e.g. government data requests), and some involuntary (e.g. cyberattacks). Those with the best access to data are the companies with which we have shared this data in a quasi-consensual manner, and the third parties with which they subsequently share the data, and the governments that are able to persuade or coerce the companies to turn over this data to them, and the domestic and foreign governments that are able to monitor

communications and hack into computers, and the perpetrators and beneficiaries of successful cyberattacks that precipitate massive data leaks. At present, those with the best access to user data are not the individuals themselves or researchers and public interest organizations. Instead, it is those in a position to monetize this data, those with the weight of government behind them, or those that are able to steal this data. Despite recent efforts by Google and others to allow users to peruse and download their own data, individuals typically have a more difficult time gaining access. Researchers and non-profit organizations who would put this data to good use (most of them, anyway) are hampered by the cost of acquiring privately held data and the ethical quandaries of conducting research on sensitive data. Many believe that access to this data will revolutionize research by providing a rich foundation for quantitative social science research.[3]

The possible ways for individuals to reconcile privacy with responsible data use include changing personal behaviors to better protect personal data and avoiding platforms that are known to be aggressive about collecting data, sloppy in protecting this data, and promiscuous in sharing data with third parties. This is an impractical option for most, as this would entail no longer using many of the most useful services and platforms. Another factor is that users are not in a position to fully and accurately evaluate how well companies protect their privacy and security. Bruce Schneier describes this asymmetric user-company relationship as "digital feudalism," in the sense that the privacy and security of users is tied to the decisions of their providers, over which they have no power and little knowledge.[4] There are a growing number of tools to help users better protect their data, and efforts are ongoing to shore up the security of core Internet infrastructure. Currently, the only surefire way to protect one's digital privacy is to opt out entirely.

Persuading or requiring companies to adopt better data management practices is another approach, and technological advances may play a supporting role. However, the current economic foundation of the Internet (non-subscription services that monetize data they collect coupled with a reluctance of users to pay for privacy enhancing services) is a serious impediment. Most companies are not motivated to minimize data collection and sharing since they rely on it as their primary source of revenue. New technologies, which provide better methods for preserving privacy and confidentiality in the context of sharing data and analysis, may offer companies tools to limit exposure and access by third parties while retaining the data's commercial viability. Emerging theoretical approaches such as Differential Privacy have shown promise in this regard,[5] but they have not yet been successfully implemented in practice at scale. Compounding lack of incentives and tools is that many companies have been slow to allocate the resources necessary to protect data from cyberattacks. If the frequency and impact of cyberattacks continue to increase over time, as they have over the last decade,[6] companies will be forced to invest more to harden their infrastructure against cyberattacks. It remains to be seen whether this will succeed in turning back the tide.

The remaining option is the imposition of stronger legal protections. One way forward would be to give even greater power to regulators and authorities to help guide the collection and use of data, potentially through third party auditors. The European Union seems to be following this path; meanwhile the United States has yet to alter its sectorial framework, leaving much of the data collected by Internet companies subject only to self-regulation. However, it is still unclear whether legal and regulatory remedies would achieve a better balance between the competing interests. Another approach would be to offer incentives to companies to take on heightened responsibility for the proper handling

of user data, shifting the role of companies to also encompass that of "information fiduciaries."[7] In all likelihood, no single solution will solve the many complex dimensions of today's privacy problems. Hybrid models in which approaches are combined and stakeholders from government and industry partner together may be necessary. In most places around the world, the clarity of purpose and political will to enact significant change are still lacking. A test for the coming years will be whether the diminishing online privacy is transformed into political action, a change in business models or company practices, or a shift in consumer behaviors.

Notes

1 Lauren Paul Gibbons, "It's the world's biggest copy machine—watch out," PC Week, January 27, 1997, https://web.archive.org/web/19990506002945/http://www.zdnet.com/pcweek/business/0127/27copy.html.

2 Victor Mayer-Schönberger and Kenneth Cukier, Big Data: A Revolution that will Transform How We Live, Work, and Think (New York: Houghton Mifflin Harcourt, 2013).

3 Gary King, "The Changing Evidence Base of Social Science Research," in Gary King, Kay Scholzman, Norman Nie, eds., The Future of Political Science: 100 Perspectives (New York: Routledge Press, 2009).

4 Bruce Schneier, "Power in the Age of the Feudal Internet," Internet Monitor 2013: Reflections on the Digital World, December 2014, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2366840.

5 Cynthia Dwork, "Differential Privacy for Everyone," Microsoft Research 2012, download.microsoft.com/download/D/1/F/D1F0DFF5-8BA9-4BDF-8924-7816932F6825/Differential_Privacy_for_Everyone.pdf.

6 Verizon Enterprise, 2014 Data Breach Investigations Report (April 2014), http://www.verizonenterprise.com/DBIR/2014/.

7 Jonathan Zittrain, "Facebook Could Decide an Election Without Anyone Ever Finding Out," The New Republic, June 1, 2014, http://www.newrepublic.com/article/117878/information-fiduciary-solution-facebook-digital-gerrymandering; Jack Balkin, "Information Fiduciaries in the Digital Age," Balkinization, March 5, 2014, http://balkin.blogspot.co.uk/2014/03/information-fiduciaries-in-digital-age.html.

Data Revolutions: Bottom-Up Participation or Top-Down Control?

Tim Davies

In September 2015, through the United Nations, governments will agree upon a set of new Sustainable Development Goals (SDGs) replacing the expired Millennium Development Goals and setting new globally agreed targets on issues such as ending poverty, promoting healthy lives, and securing gender equality.[1] Within debates over what the goals should be, discussions of online information and data have played an increasingly important role.

Firstly, there have been calls for a "Data Revolution" to establish better monitoring of progress towards the goals: both strengthening national statistical systems and exploring how "big data" digital traces from across the Internet could enable real-time monitoring.[2] Secondly, the massive United Nations-run MyWorld survey, which has used online, mobile, and offline data collection to canvas over 4 million people across the globe on their priorities for future development goals, consistently found "An honest and accountable government" amongst people's top five priorities for the SDGs.[3] This has fueled advocacy calls for explicit open government goals requiring online disclosure of key public information such as budgets and spending in order to support greater public oversight and participation.

These two aspects of "data revolution" point to a tension in the evolving landscape of governments and data. In the last five years, open data movements have made rapid progress spreading the idea that government data (from data on schools and hospitals locations to budget datasets and environmental statistics) should be "open by default": published online in machine-readable formats for scrutiny and re-use. However, in parallel, cash-strapped governments are exploring the greater use of private sector data as policy process inputs, experimenting with data from mobile networks, social media sites, and credit reference agencies amongst others (sometimes shared by those providers under the banner of "data philanthropy"). As both highly personal and commercially sensitive data, these datasets are unlikely to ever be shared en-masse in the public domain, although this proprietary data may increasingly drive important policy making and implementation.

In practice, the evidence so far suggests that the "open by default" idea is struggling to translate into widespread and sustainable access to the kinds of open data citizens and civil society need to hold powerful institutions to account. The multi-country Open Data Barometer study found that key accountability datasets such as company registers, budgets, spending, and land registries are often unavailable, even where countries have adopted open data policies.[4] And qualitative work in Brazil has found substantial variation in how the legally mandated publication of spending data operates across different states, frustrating efforts to build up a clear picture of where public money flows.[5] Furthermore, studies regularly emphasize the need not only to have data online, but also the need for data literacy and civil society capacity to absorb and work with the data that is made available, as well as calling for the creation of intermediary ecosystems that provide a bridge between "raw" data and its civic use.

Over the last year, open data efforts have also had to increasingly grapple with privacy questions.[6]

Concerns have been raised that even "non-personal" datasets released online for re-use could be combined with other public and private data and used to undermine privacy.[7] In Europe, questions over what constitutes adequate anonymization for opening public data derived from personally identifying information have been hotly debated.[8]

The web has clearly evolved from a platform centered on documents to become a data-rich platform. Yet, it is public policy that will shape whether it is ultimately a platform that shares data openly about powerful institutions, enabling bottom up participation and accountability, or whether data traces left online become increasingly important, yet opaque, tools of governance and control. Both open data campaigners and privacy advocates have a key role in securing data revolutions that will ultimately bring about a better balance of power in our world.

Notes

1 UN High-Level Panel of Eminent Persons on the Post-2015 Development Agenda, "A New Global Partnership: Eradicate poverty and transform economies through sustainable development," 2013, http://www.un.org/sg/management/pdf/HLP_P2015_Report.pdf.
2 Independent Expert Advisory Group on the Data Revolution, http://www.undatarevolution.org.
3 MyWorld Survey, http://data.myworld2015.org/.
4 World Wide Web Foundation, "Open Data Barometer," 2013 (and 2014, forthcoming), http://www.opendatabarometer.org.
5 N. Beghin and C. Zigoni, "Measuring open data's impact of Brazilian national and sub-national budget transparency websites and its impacts on people's rights," 2014, http://opendataresearch.org/content/2014/651/measuring-open-datas-impact-brazilian-national-and-sub-national-budget.
6 Open Data Research Network, "Privacy Discussion Notes," 2013, http://www.opendataresearch.org/content/2013/501/open-data-privacy-discussion-notes.
7 Steve Song, "The Open Data Cart and Twin Horses of Accountability and Innovation," June 19, 2013, https://manypossibilities.net/2013/06/the-open-data-cart-and-twin-horses-of-accountability-and-innovation/.
8 See the work of the UK Anonymisation Network, http://ukanon.net/.

Everything is Data. Yes, Even Development.

Malavika Jayaram

Recent revelations about pervasive data collection and processing have revealed a discomfiting nexus between the government and corporations. Consequently, the push for surveillance reform has largely been directed at the state, on one hand, and at large Internet and telecommunications companies, on the other. There are, however, serious threats to privacy and other civil liberties from another seemingly benign source: the matrix of organizations enacting and implementing development and welfare the world over.

Several factors are at play here. The desire to transform governance and civic participation can galvanize Internet penetration, the digitization of bureaucratic processes, and the roll-out of electronic voting schemes. Policy goals of financial inclusion and poverty alleviation often legitimize national identity projects and credit rating systems (especially when framed as essential architecture for fraud-resistant commerce). The frustration with endemic corruption and crony capitalism drives movements towards transparency and open government. Advances in technology trigger innovations in crisis mapping, healthcare, public transport, energy, water management, and agriculture.

Despite the worthiness of these schemes and the grave societal concerns that they seek to address, a common yet critical flaw may compromise or subvert them. By design or incidentally, they deal in massive quantities of personal data, yet—because they do not see themselves as data gathering projects necessarily—many of them have poor privacy and security practices. This is not surprising: they are largely designed and implemented by development specialists, not technologists and lawyers. Larger NGOs or global organizations may approach data privacy and operational security with caution and rigor; smaller, less sophisticated agencies and their floating pools of researchers and volunteers may not.

Extremely sensitive data may be gathered in contexts that are problematic, calling into question the role of power imbalances, the lack of agency, the inability to provide genuine informed consent, and the desperate circumstances that render the so-called "privacy bargain" meaningless. Even where these ethical considerations are mapped out and addressed, the data may be stored, disseminated, combined with other data, or used in ways that are privacy-invasive or just plain insecure. Commitments to open up data, whether mandated by funders, governments, academic institutions, or organizational values, can result in the publishing of identifying information rather than aggregated, anonymized data. Resource constraints may force the use of insecure platforms and services for communications and storage. Above all, the lack of awareness makes all of these possibilities real and widespread.

It used to be that the 'privacy paranoiacs' and the 'open evangelists' rarely interacted. In a post-Snowden universe, they have begun to engage in a critical conversation about positive-sum games and middle grounds, mapping ways to minimize the discriminatory effects of algorithmic bias, social sorting, and disparate impact. Equally importantly, the need for a cross-disciplinary approach to responsible data ethics has gained traction, pulling together security experts, civil society actors, data

scientists, healthcare professionals, and other subject matter experts. This may not halt the emergence of a "welfare-industrial complex" of policymakers, technology vendors, welfare agencies, and law enforcement that takes surveillance into the development arena. It may, however, stem the disconnect between data and people, between statistics and lived experiences. Zygmunt Bauman talks of one person's civilizing process being another person's forceful incapacitation.[1] By having a more nuanced conversation about the surveillance potential of the (often paternalistic) development sector, we may yet move beyond the chilling "If you're not counted, you don't count" rhetoric that underpins so many development efforts today.

Notes

1 Zygmunt Bauman, Life in Fragments: Essays in Postmodern Modernity (Oxford: Blackwell, 1995).

Mapping the Data Ecosystem

Sara M. Watson

What would it take to map the Internet? Not just the links, connecting the web of sites to each other, or some map of the network of networks. That's hard enough in itself.

What if we were to map the flows of data around the Internet? Not just delivering packets, but what those packets contain, where they propagate, how they are passed on, and to what ends they are used.

Between our browser history, cookies, social platforms, sensors, brokers, and beyond, there are myriad parties with economic interests in our data. How those parties interconnect and trade in our data is, for the most part, opaque to us.

The data ecosystem mirrors the structure of the Internet. No single body has dominion or a totalizing view over the flows of information. That also means that no one body is accountable for quality or keeping track of data as it changes hands and contexts.

Data-driven companies like Facebook, Google, Acxiom, and others are building out their proprietary walled gardens of data. They are doing everything they can to control for privacy and security while also keeping control over their greatest assets. Still, they aren't held accountable for the ads individuals purchase and target on their platforms, or for tertiary uses of data once it leaves their kingdom.

Complexity obscures causality. So many variables are fed into the algorithm and spit back out on a personalized, transient platform that no one can tell you exactly why you saw one post over another one in the feed or that retargeted ad over this one. We conjure up plausible explanations and grasp at folk theories that engineers offer up to explain their outputs.

We have given data so much authority without any of the accountability we need to have confidence in its legitimacy to govern our lives.

As everything, refrigerators and crockpots included, expand the Internet and the ecosystem of data that runs on top of it, everything will leave a data trail. Going forward we have to assume that what can be codified and digitized will become data. What matters is how that data will be used, now and in the future.

The potential harms are hard to pin down, primarily because we won't know when they are happening. We can't investigate discrimination that replaces pre-digital prejudice markers like race and sex with proxies correlated from behavioral data. And we run into invisible walls based on statistical assumptions that anticipate our needs but get us wrong if we fall outside the curve. It's nearly impossible to catch these slights and even harder to develop normative stances on grounds we cannot see.

Before we can start to discuss normative judgments about the appropriate uses of data, we have to

understand the extent of what is technically possible. We cannot hope to regulate the misuse of data without means to hold all interconnected parties accountable for the uses and flows of data.

We need to map these relationships and data patterns. Who are the parties involved? How are they collecting, cleansing, inferring and interpreting data? To what ends is the data being used?

Linked Data is one technical solution to this problem. Standards make data flows both machine readable and human legible. Policies that travel as metadata are another approach to distributed accountability. We can also hold some of the largest brokers and users of data to higher standards of ethics. But markets of users won't move against these systems until we have a better map of the ecosystem.

Mapping the Next Frontier of Open Data: Corporate Data Sharing

Stefaan G. Verhulst and David Sangokoya

When it comes to data, we are living in the Cambrian Age. About ninety percent of the data that exists today has been generated within the last two years. We create 2.5 quintillion bytes of data on a daily basis—equivalent to a "new Google every four days."[1]

Among the staggering statistics illustrating today's rapid generation and volume of data, the number of mobile phone subscriptions is expected to reach 7 billion by the end of 2014, nearly equal to the world's population.[2] Terabyte after terabyte of data and metadata from these 7 billion mobile subscriptions is collected and stored by corporations. Given the amount of mobile, social, and digital data available, corporations have access to a wealth of consumer data on their servers that can be aggregated and analyzed to track preferences, provide more targeted consumer experiences, and derive value towards the corporate bottom line.

As we witness the rapid intensification of "datafication," access to data is growing increasingly critical and essential to addressing many of our most important social, economic, and political challenges. While the rise of the Open Data movement has opened up over a million datasets largely from government agencies and departments, data held by corporations has been harder to access. Most companies are unwilling to share the data they are collecting due to concerns over the legal ramifications of privacy and security breaches—as well as trade secrets and proprietary interests.

At the same time, we witness several early attempts by corporations to open up their datasets for analysis by researchers, public interest organizations, and third parties to inform decision-making. By combining original datasets from corporate data providers with diverse, geo-spatial datasets (such as open government data and open science data), users can uncover greater insights and correlations across a range of societal trends.

Corporate data sharing refers to the emerging trend whereby companies are sharing anonymized and aggregated data for third-party users to mine for patterns and trends that can inform better policies and lead to greater public good. The trend was originally coined "corporate data philanthropy" at the World Economic Forum meeting in Davos in 2011 and has gained wider currency through Global Pulse, a United Nations data project that has popularized the notion of a global "data commons."[3] In what follows, we share early findings of our efforts to map this new frontier of open data, along with a set of research questions that must be addressed to understand the value of corporate data sharing better. Illustrating the practice and assessing the importance of opening corporate data will be necessary to accelerate increased access to societally valuable data held by business today.

Taxonomy of current corporate data sharing practices

For all the growing attention corporate data sharing has recently been receiving, it remains very much a fledgling field. Much remains to be defined and understood. There has been little rigorous analysis of different ways of sharing, though our initial mapping of the landscape resulted in identifying six

main categories of activity to date:

1. Research partnerships, in which corporations share data with universities and other research organizations. Through partnerships with corporate data providers, several research organizations are conducting experiments using anonymized and aggregated samples of consumer datasets and other sources of data to analyze social trends. For instance:

- Yelp shares its data on neighborhood businesses with 30 universities for researchers to build tools and discover meaningful value in the data. Using shared data on Yelp businesses in the San Francisco Bay Area, an academic research team from UC Berkeley used a probabilistic model for natural language processing to detect subtopics across a dataset of over 200,000 Yelp business reviews. Their research uncovered correlations between positive ratings and service quality, giving business owners evidence for improving their services.[4]
- Collecting over 20 terabytes of data per month through satellite imagery, Intel is partnering with researchers at the University of California at Santa Barbara to map snow patterns in the Sierra Nevada mountains and understand California's remaining water resources.[5]
- Safaricom, one of Kenya's leading mobile companies, shared a year of anonymized phone data with Harvard researchers to map how migration patterns contributed to the spread of malaria in Kenya. By combining Safaricom's data on call locations with national infectious disease data, researchers were able to estimate and map routes that contributed to the spread of the disease.[6]
- Just recently, online communities like Imgur and Reddit have joined forces with a select group of academic institutions as part of the Digital Ecologies Research Partnership (DERP) in order to provide data and support research on Internet social behavior.[7]

2. Prizes and challenges, in which companies make data available to qualified applicants who compete to develop new apps or discover innovative uses for the data. Companies typically host these contests in an effort to incentivize a wide range of civic hackers, pro-bono data scientists, and other expert users to find innovative solutions with the available data. For instance:

- In Ivory Coast and Senegal, Orange Telecom hosted a global challenge that allowed researchers to use anonymized, aggregated data to help solve various development problems, including those related to transportation, health, and agriculture.[8]
- In its 2014 Dataset Challenge, Yelp is making its data on restaurants in cities like Phoenix, Madison, and Edinburgh available to academic researchers to build models and provide research on urban trends and behavior (such as whether Yelp data can help predict environmental conditions of restaurants).[9]
- Last year, Spain's regional bank BBVA hosted a contest inviting developers to create applications, services, and content based on anonymous card transaction data. The first prize went, for instance, to an application called Qkly, which helps users plan their time by estimating what time of day a given place will be most overcrowded so as to avoid

lines.[10]

- In its "Big Data Challenge," Telecom Italia pooled its data with partners from various Italian industries (local news, automobile, energy and weather) into one aggregated, geo-referenced dataset for participants to use for the competition. The data was available in batches and through an API, and contained millions of call data records, energy consumption records, tweets, and weather data points.[11]

3. Trusted intermediaries, where companies share data with a limited number of known partners. Companies generally share data with these entities for data analysis and modeling, as well as other value chain activities. For instance:

- South Africa-based telecom MTN makes anonymized call records available to researchers through a trusted intermediary, Real Impacts Analytics—a data analytics firm that provides guided and predictive analytics solutions.[12]
- Twitter recently acquired the social media aggregator Gnip in order to provide its data products to clients. Gnip allows Twitter to provide streams of its dataset to its clients in addition to streams from available social media data.[13]

4. Application programming interfaces (APIs), which allow developers and others to access data for testing, product development, and data analytics. By signing a terms of service agreement, users receive access to streams of data from companies in order to build applications. For instance:

- Through its metadata and click tracking functionality, Bitly estimates social trends and allows users to build tools from real-time data.[14]
- Building on top of its transportation data, Uber recently shared its API with companies such as Hyatt, United Airlines, and Smart Calendar in order to integrate its services across related industries and improve overall customer experience.[15]

5. Intelligence products, where companies share (often aggregated) data that provides general insight into market conditions, customer demographic information, or other broad trends. For instance:

- Google shares search query-based data in conjunction with data from the US Centers for Disease Control in order to estimate levels of influenza activity over time.[16]
- Facebook Open Graph Search allows consumers and companies to mine social graphs for search query-based data, such as demographic and location data, "likes," and multimedia. Companies such as Slate and Upworthy have used available data from Open Graph Search to optimize their headlines and increase readership.[17]

6. Corporate Data cooperatives or pooling, in which corporations—and other important dataholders such as government agencies—group together to create "collaborative databases" with shared data resources. These collaborations typically require an organizing partner as well as technical and legal frameworks surrounding the use and distribution of the data. For instance:

- Recently, the White House has announced the development and launch of a data public-private partnership, which will involve making existing climate data, tools and products more accessible to decision-makers.[18]
- Through its Accelerating Medicines Partnership, the US National Institutes of Health (NIH) is helping organize data pooling among the world's largest biopharmaceutical companies in order to identify promising drug and diagnostic targets for Alzheimer's disease.[19]

Mapping the next frontier

Beyond such broad taxonomies, there exists almost no systematic analysis of corporate data sharing. Much research remains to be done on the value proposition for corporations doing the sharing (or, indeed, for end users), and on ways to maximize the potential and—importantly—minimize potential harms of shared data.

A more comprehensive mapping of the field of corporate data sharing would draw on a wide range of case studies and examples to identify opportunities and gaps, and to inspire more corporations to allow access to their data (consider, for instance, the GovLab's Open Data 500 mapping for open government data). From a research perspective, the following questions would be important to ask:

- What types of data sharing have proven most successful, and which ones least?
- Who are the users of shared corporate data, and for what purposes?
- What conditions encourage companies to share, and what are the concerns that prevent sharing?
- What incentives can be created (economic, regulatory, etc.) to encourage corporate data sharing?
- What differences (if any) exist between shared government data and shared corporate data?
- What steps need to be taken to minimize potential harms (e.g., to privacy and security) when sharing data?
- What's the value created from using shared corporate data?

Additional Reading

Pawelke, Andreas and Anoush Rima Tatevossian. "Data Philanthropy: Where Are We Now?," UN Global Pulse Blog, May 8, 2013, http://www.unglobalpulse.org/data-philanthropy-where-are-we-now.

Stempeck, Matt. "Sharing Data Is A Form Of Corporate Philanthropy," Harvard Business Review, July 24, 2014, http://blogs.hbr.org/2014/07/sharing-data-is-a-form-of-corporate-philanthropy.

Verhulst, Stefaan. "Mapping The Next Frontier Of Open Data: Corporate Data Sharing," The Govlab Blog, September 16, 2014, http://thegovlab.org/mapping-the-next-frontier-of-open-data-corporate-data-sharing.

Notes

1 IBM and Paul Zikopoulos, Understanding Big Data, 1st ed. (New York: McGraw-Hill, 2012).

2 ITU, "World Telecommunication/ICT Indicators Database," 2014, http://www.itu.int/en/ITU-D/Statistics/Pages/publications/wtid.aspx.

3 Robert Kirkpatrick, "A New Type Of Philanthropy: Donating Data," Harvard Business Review, March 21, 2013, http://blogs.hbr.org/2013/03/a-new-type-of-philanthropy-don/.

4 UC Berkeley School of Information, "Students' Data Analysis Uncovers Hidden Trends In Yelp Reviews," October 4, 2013, http://www.ischool.berkeley.edu/newsandevents/news/20131004yelpdatasetchallenge.
5 Lyndsey Gilpin, "How Intel Is Using Iot And Big Data To Improve Food And Water Security," Techrepublic, June 13, 2014, http://www.techrepublic.com/article/how-intel-is-using-iot-and-big-data-to-improve-food-and-water-security/.
6 Amy Wesolowski, Nathan Eagle, Andrew J. Tatem, David L. Smith, Abdisalan M. Noor, Robert W. Snow, and Caroline O. Buckee, "Quantifying the impact of human mobility on malaria," Science, October 12, 2012, http://www.sciencemag.org/content/338/6104/267.
7 Alex Hern, "Reddit, Imgur And Twitch Team Up As 'Derp' For Social Data Research," The Guardian, August 18, 2014, http://www.theguardian.com/technology/2014/aug/18/reddit-imgur-twitch-derp-social-data.
8 Vincent D. Blondel, et al., "Data for development: the d4d challenge on mobile phone data." arXiv preprint arXiv:1210.0137 (2012).
9 Yelp.com, "Yelp Dataset Challenge," http://www.yelp.com/dataset_challenge.
10 Miguel Ángel Iñesta, "BBVA On The Trail Of Its Own Applications Ecosystem," BBVA Innovation Center, December 10, 2013, http://www.centrodeinnovacionbbva.com/en/blogs/entrepreneurs/post/bbva-trail-its-own-applications-ecosystem.
11 Telecom Italia Corporate, "Bigdata Challenge," http://www.telecomitalia.com/tit/it/bigdatachallenge.html.
12 Real Impact Analytics, "Churn Prediction With Social Network Analysis," http://www.realimpactanalytics.com/blog/churn-prediction-social-network-analysis/.
13 Jana Messerschmidt, "Twitter Welcomes Gnip To The Flock," Twitter Blog, April 15, 2014, https://blog.twitter.com/2014/twitter-welcomes-gnip-to-the-flock.
14 "Announcing The Bitly Social Data APIs," Bitly Blog, January 8, 2013, http://blog.bitly.com/post/40026085295/announcing-the-bitly-social-data-apis.
15 "Introducing The Uber API," Uber Blog, August 20, 2014, http://blog.uber.com/api.
16 "Google Flu Trends | United States," http://www.google.org/flutrends/us/#US.
17 Facebook Developers, "Overview," https://developers.facebook.com/docs/opengraph/overview.
18 The White House, "FACT SHEET: President Obama Announces New Actions To Strengthen Global Resilience To Climate Change And Launches Partnerships To Cut Carbon Pollution," September 23, 2014, http://www.whitehouse.gov/the-press-office/2014/09/23/fact-sheet-president-obama-announces-new-actions-strengthen-global-resil.
19 Sara Reardon, "Pharma Firms Join NIH On Drug Development," Nature, February 4, 2014, doi:10.1038/nature.2014.14672.

The Social and Technical Tribulations of Data Privacy in a Mobile Society

Adrienne Debigare & Nathan Freitas

As the world begins to fully embrace digital communication, there are both inherent benefits and challenges in its adoption. More than ever, the Internet and Internet-enabled devices allow us nimbly to organize, mobilize, and strategize. Increasingly, we're taking that connection with us in the form of mobile devices. Indeed, mobile adoption far outpaces desktop in developing countries. But with the omnipresence that allows fluid communication are new opportunities for surveillance and tracking. Our mobile phones are essentially homing beacons, emitting GPS coordinates almost constantly to a variety of companies and organizations both known and unknown to the consumer. Through text messaging and social media we are able to stay in touch with loved ones thousands of miles away, organize action, or disseminate revelatory information at the speed of light. But these digital traces also allow oppressive governments to track a dissident's every move,[1] a jealous spouse to surreptitiously monitor their partner's phone messages,[2] or a marketer to unknowingly reveal guarded secrets about a consumer.[3] As we continue developing mobile technology, the key question is: how might we mitigate its basic security flaws and cogently minimize the leakage of data to unknown individuals and groups?

A challenge in standardizing mobile security is the lack of consumer knowledge. The interfaces for popular products naturally highlight the benefits of data gathering, while downplaying the privacy sacrificed. While Google Maps' traffic overlays have all but replaced the radio station traffic report for some, it is easy to overlook the vast number of users who are unconsciously submitting their exact location and speed to Google in order to build that accurate picture.

To combat this lack of information, privacy proponents have begun to compile user guides for secure technology use. Notably, the Electronic Frontier Foundation just completed the Secure Messaging Scorecard, a first-of-its-kind survey of a comprehensive list of messaging services, from Facebook Messenger to WeChat.[4] The list may not be surprising in its findings, but for many consumers it will make many of the "unknown unknowns" of security at least into "known unknowns."

At its core, the Scorecard asks: What makes an app secure? It identifies several touchpoints, from the very basic, such transit encryption, to the more involved, like allowing for code audits. For the technically indoctrinated, the list is a fascinating first look into the nuances of various communication clients, and for the global NGOs, activists, and journalists the list will become especially indispensable.

But the ubiquity of some of the most insecure apps (i.e., Facebook Messenger, Skype, and Google Hangouts) on the list demonstrates how low consumer demand for security—limited to the few aforementioned circles—truly is. Upon further investigation, it becomes easier to understand why the Facebook-and-email mobile user might seem lackadaisical. In the methodology section, there are many references to "endpoints," "user keys," and other cryptographic jargon which can feel opaque and confusing to the casual user.

For example, one question on the Scorecard, "Can you verify contacts' identities," seems utterly inapplicable to the "average" consumer, who knows every person in their phone's address book. But this question actually refers to a hacker's ability to essentially trick an app into thinking it is communicating with a trusted source, and then stealing or re-routing any information the user enters. China was recently caught doing this to Chinese citizens' iCloud accounts.[5]

It is in this dense and complicated verbiage that privacy activists and the public find the chasm separating them. In a now-famous June 2014 TV segment, John Oliver mocked the term 'net neutrality' for being boring.[6] In the same way, many of the terms that come second nature to privacy groups are either misconstrued or off-putting to the public at large.

However, mobile messaging service WhatsApp might be a signal of a changing tide. Recently, the company announced their partnership with Open Whisper Systems to introduce end-to-end encryption.[7] End-to-end encryption is the envelope to a non-secure message's postcard. While it may not solve the problem of back doors or security holes, it at least ensures a message's journey will be uninterrupted by prying eyes.

Admittedly, the move by WhatsApp translates to little more than Google introducing https into Gmail. In 2010, Google announced a move to full adoption of the secure protocol that would protect email data from computer to server, from an opt-in model that was rolled out in 2008.[8] It hasn't protected Gmail users from NSA or even Google surveillance, but it was also a relatively simple implementation that caused little customer pain. Like Google, WhatsApp's decision to encrypt traffic has had little effect on the customer's daily use of the product, and the press surrounding the move may be enough to spark conversations among a mainstream audience and bring attention needed cultural shifts. In this way, even a rudimentary technical upgrade can have much larger societal impact.

We as a society are still continuing to chart dark waters in the field of digital security. The complacent adoption of surveillance devices is surely not what casual users think about when purchasing the latest mobile device, but it is imperative that privacy activists find shared ground and open accessible conversation around mobile security. The major challenge is that users, at best, don't understand the need for complex security systems and, at worst, demonize these measures as the realm of criminals and terrorists. The greatest progress to be made in the near future is less about the development of new technologies, and more about social buy-in to these paradigms.

Notes

1 "Era of the Digital Mercenaries," Reporters Without Borders, http://surveillance.rsf.org/en/.
2 Stealth Genie Review, http://www.stealthandroidspy.com/.
3 Charles Duhigg, "How Companies Learn Your Secrets," New York Times, February 19, 2012, http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.
4 "Secure Messaging Scorecard," Electronic Frontier Foundation, https://www.eff.org/secure-messaging-scorecard.
5 Paul Mozur, Nicole Perlroth, and Brian X. Chen, "Apple's iCloud Storage Service is Aim of Attack in China," New York Times, October 22, 2014, http://www.nytimes.com/2014/10/22/technology/china-attack-aims-at-apple-icloud-storage-service.html.
6 Terrance F. Ross, "How John Oliver Beats Apathy," The Atlantic, August 14, 2014, http://www.theatlantic.com/entertainment/archive/2014/08/how-john-oliver-is-procuring-latent-activism/376036/.
7 "Open Whisper Systems partners with WhatsApp to provide end-to-end encryption," Open Whisper Systems Blog, November 18, 2014, https://whispersystems.org/blog/whatsapp/.
8 Sam Schillace, "Default https access for Gmail," Official Gmail Blog, January 12, 2010, http://gmailblog.blogspot.com/2010/01/default-https-access-for-gmail.html.

The Future of the Internet—and How to Secure It

Andy Ellis

Once, there was an Internet. And it was a happy place with no security concerns whatsoever, because only a dozen or so people got to use it.

That fairy tale is not the world we live in today, and thanks to high profile problems like Heartbleed and Shellshock, more people recognize it. Unfortunately, some of the design ethos from that fantasyland still impacts us. The web isn't secure for the uses it sees today—and HTTP was never designed to be. SSL, intended to provide a secure connection layer between systems, has evolved through multiple versions into TLS, each attempting to reduce the vulnerabilities of the prior. The vulnerabilities and problems of HTTPS, while not numberless, are legion. And each of these vulnerabilities presents an opportunity for an adversary to defeat the goals of Internet users—whether they seek financial security, privacy from government surveillance, or network agnosticism.

What is HTTPS, anyway?

HTTPS isn't a standalone protocol; HTTP over TLS is two separate protocols, isolated from one another. The effects of one protocol's actions on another are rarely studied as much as the actual protocols themselves. That isolation has led to vulnerabilities—using compression in HTTP to improve transfer speed is good, except that the secrecy goals of TLS can be subverted through variable-sized content, as in the BREACH security exploit.

Who do you trust?

TLS certificates are issued by certificate authorities (CAs); these CAs sign the certificates that a web site presents to its users to 'prove' who they are. You could almost consider them like a driver's license—issued by some authority. But who are these authorities? They are the dozens of entities—some commercial, some governmental—who are trusted by our browsers. Unlike a driver's license, any trusted CA can issue a certificate for any website—it's like having your local library issue an ID card for a Pentagon employee or one government issue certificates for another government's website.

Illegitimately gaining a trusted certificate can be achieved through at least three distinct paths:

- compromise a CA publishing interface, either directly or by compromising a user's credentials;
- for Domain Validated certificates, have publication control of the website that the CA can observe (by compromising DNS, the publication interface, or the server directly); or
- by modifying the browser's list of trusted certificates. This is a common practice in many enterprises, to enable the enterprise to run a CA for their own websites, or to deploy a web filtering proxy. But these CAs are then able to issue certificates to any website.

Once an adversary has a certificate, they merely need to also become a 'man in the middle' (MITM), able to intercept and modify traffic between a client and a server. With this power set, they are able to read and modify all traffic on that connection.

Certificate Transparency (CT) is an initiative to begin monitoring and auditing the CAs to determine whether they have issued rogue certificates and to provide browsers an interface to collectively validate certificates. This may lead to a reduction in the number of trusted CAs to only those that don't behave in a rogue fashion. There is another possible mitigation called DANE (DNSSEC Assertion of Named Entities), where the information about the validity of certificates/authorities for hostnames/domains is published through DNS and signed by DNSSEC, reducing the number of trusted entities who can publish SSL keys.

I can haz TLS?

Until recent versions of TLS that incorporate Server Name Indication (SNI), a server was required to first present the certificate that declared for which hosts it was able to conduct an HTTPS session. This meant that no IP address could have more than one certificate. In HTTP, a single IP address can, through virtual hosting, have many hostnames, as the client will signal to the server which hostname from which it would like a web page. While the advent of multi-domain certificates has allowed multiple hostnames, it hasn't provided the freedom to have 'unlimited' TLS-secured hostnames. SNI is an extension to TLS that provides this capability, allowing a browser to tell a server what certificate it would like to be presented.

But SNI isn't supported by all browsers—most notably, Windows XP and early versions of Android. The former is on its way out, but the latter is still being deployed on lower-end feature phones, especially in the developing world. And unfortunately, there are no good strategies for supporting both SNI and non-SNI clients available today. Until either SNI is fully supported, or IPv6 adoption achieves critical mass, many websites will not be able to have HTTPS.

TLS is only Transport Layer Security

Often, a client isn't talking directly to the content provider—there is some other entity in the middle. It might be an enterprise proxy; it might be a network operator gateway; it might be a content delivery network. In these cases, the TLS connection only provides secrecy on the first leg—the client has to hope that the secrecy is preserved across the public Internet. Few of the mid-point entities provide any assertions about how they'll handle the security of the forward connections that were prompted from a TLS connection; some even advertise the convenience of having the 'flexibility' to downgrade from HTTPS to merely HTTP.

Until HTTP contains a signaling mechanism through which the mid-points can communicate about the TLS choices they've made, a client will not know whether a TLS connection is robust (or even exists!) across public links.

TLS isn't privacy

TLS provides encryption for the information contained inside a request, thus hiding the specific content you're engaging with. It's useful for hiding the specific details of similarly shaped data, like social security numbers or credit cards; but very poor at hiding things like activism or research. The design of the system doesn't conceal the 'shape' of your traffic—and the Wikipedia pages for Occupy Central have a different shape than the shape of the Wikipedia page for the Large Hadron Collider. It also doesn't prevent traffic analysis—while the contents of a user-generated video may be secret, the identity of the systems (and hence the users) that uploaded and downloaded it aren't. Some privacy systems like Tor may provide useful protections, but at the cost of performance.

Don't trust the lock

All together, the architecture of TLS and HTTPS doesn't provide enough safety against all adversaries in all situations. There are some steps underway that will improve safety, but many hazards will still remain, even absent the highly publicized implementation defects. But these steps will increase the cost for adversaries, sometimes in measurable and observable ways.

That icon lock in your browser is useful for securing your commerce and finances, but be cautious about trusting it with your life.

Data Protection and Privacy Law: Where Regulators Are King?

Neal Cohen

Across the world, data protection and privacy law is in a phase of rapid growth. As we move closer to the Internet of things, living in a world of wearable tech, smart homes, and smart cities, where every device is potentially personal and at the same time universal, society must decide on what rules should govern this world. What information should be considered personal data? What requirements should be in place regarding the collection, use, and sharing of personal data, and what activities should be prohibited? What does it mean for an individual to express consent, and when is affirmative or explicit consent required? The answers to these questions shape the world in which we live.

As data protection and privacy law is still very much in its infancy, the aforementioned questions pose challenges for companies and regulators alike. Both companies and regulators need binding law to guide their actions—law that reflects the will of society. Companies need to know what data processing activities are lawful, and regulators need to know when enforcement is appropriate.

At present, much of the world is going through legislative reform in regards to data protection and privacy law in an effort to help address those questions.[1] However, in the absence of clear legislation or court decisions, regulators frequently publish non-binding guidance to fill the gap. This non-binding guidance is needed and useful for informing companies how regulators are going to enforce the law, but it is often broad and, sometimes, beyond the scope of the law. Unless companies are willing to challenge such guidance and subsequent regulator enforcement in court, non-binding guidance is frequently treated as de facto law.

In Europe, non-binding guidance most often comes from the European Commission's Article 29 Working Party[2] and various Member State data protection authorities.[3] In recent years, these institutions have provided guidance on what information constitutes personal data,[4] what constitutes effective consent,[5] when consent is and is not required,[6] and many other similar topics. With few clarifying court decisions, these guidance documents have been treated as de facto law, as limited alternatives exist.

In the US, the Federal Trade Commission (FTC) has engaged in de facto regulation on the basis of a general prohibition against unfair and deceptive trade practices[7]—an activity that is currently being tested by the courts.[8] Through workshops,[9] non-binding guidance,[10] and, most effectively, private settlements with companies following formal complaints,[11] the FTC has established de facto requirements without promulgating privacy rules pursuant to the Administrative Procedures Act[12] and without much legal precedent to support its interpretations.

Where no sufficiently clear law exists or where such law does exist but is silent on vital nuance, is it right for a regulator to step into the shoes of a legislature or court by providing non-binding guidance on how personal data should be regulated, and more importantly, guidance on how we communicate with one another in an interconnected world? Surely this guidance is helpful, but in the absence of binding law, at what point does non-binding guidance become the law?

Notes

1 In the last few years alone, new laws have been introduced in Singapore, Uruguay, South Korea, Mexico, Malaysia and many others, and reform is ongoing across Europe, South Africa, and the United States.

2 The Article 29 Working Party is comprised of representative members of all Member State data protection regulators in the EU; see European Commission's Article 29 Working Party Opinions, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm.

3 See European Commission: National Data Protection Authorities, http://ec.europa.eu/justice/data-protection/bodies/authorities/eu/index_en.htm.

4 See Article 29 Working Party Opinion 216 on Anonymisation Techniques, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

5 See Article 29 Working Party Opinion 187 on the Definition of Consent, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf.

6 See Article 29 Working Party Opinion 217 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.

7 See Section 5 of the Federal Trade Communications Act, 15 U.S.C. §45, http://www.law.cornell.edu/uscode/text/15/45.

8 See FTC v. Wyndham Worldwide Corp., 2014 BL 94785, D.N.J., No. 2:13-cv-01887, 4/7/14, http://epic.org/privacy/big-data/ftc-v-wyndham-opinion.pdf; see also Bloomberg BNA: 3rd Circuit to Wade Into Wyndham-FTC Fight; First Appeals Court to Rule on FTC, available at http://www.bna.com/3rd-circuit-wade-n17179893179/.

9 See Federal Trade Commission: Events for a list of past and upcoming workshops and events, http://www.ftc.gov/news-events/events-calendar/all.

10 See Federal Trade Commission: Bureau of Consumer Protection, Business Center for access to FTC guidance documents, http://www.business.ftc.gov/.

11 See Federal Trade Commission: Enforcing Privacy Promises for a detailed list of past settlements, http://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises.

12 See Administrative Procedures Act, 5 U.S.C. §553, http://www.law.cornell.edu/uscode/text/5/553.

Toward a New Approach to Data Protection in the Big Data Era

Alessandro Mantelero

The complexity of data processing, the power of modern analytics, and the transformative use of personal information drastically limit the awareness of consumers about how their data is collected and used, diminish their capability to evaluate the consequences of their choices, and preclude their ability to give free and informed consent. Moreover, market concentration and related social and technological lock-ins often exclude an effective negotiation of personal information.

These elements lead us to reconsider the role of user's self-determination in data processing and the "notice and consent" model.

My suggestion is not to change the entire traditional model of data protection, but to reshape it with regard to the big data context, where asymmetries in data negotiation drastically reduce users' self-determination.

From this perspective, in the following paragraphs I propose a new model for big data uses, which is based on two fundamental pillars: the definition of a rigorous multiple impact assessment of data processing, widely adopted and publicly available, and the adoption of an "opt-out" scheme.
In the presence of complex data collection and processing systems influenced by lock-in effects, such an impact assessment should not be conducted either by consumers, or by companies. It should be conducted by third parties, under the supervision of national data protection authorities (hereafter DPAs) that define the professional requirements of these third parties.

DPAs, rather than users, have the technological knowledge to evaluate the risks associated with data processing and are in the best position to balance the interests of different stakeholders.

In the suggested model, companies that intend to use big data analytics should undergo an assessment prior to collecting and processing data. The assessment would not only focus on data security, but also consider the social impact and ethical use of data in a given project.

The entire system would work only if the political and financial autonomy of DPAs from both governments and corporations is guaranteed. Moreover, DPAs would need new competence and resources in order to bear the burden of the supervision and approval of these multiple-impact assessments.
In the light of the above, a model based on mandatory fees—paid by companies when they submit their requests for authorization to DPAs—would be preferable. This solution provides proportionate resources to authorities without being influenced by the companies under their supervision.

It should also be noted that, in cases of large scale and multinational data collection, forms of mutual assistance and cooperation may facilitate the role played by DPAs in addressing the problems related to the dimensions of both data collection and data gatherers.

However, wider cooperation at global level is difficult to realize, despite the presence of international

fora, in which the issues related to data protection are discussed (e.g. APEC, Council of Europe),. This is due to the absence of an effective common legal framework and the presence of cultural and legal differences that often affect social and ethical assessments.

Finally, with regard to the decision-making process, a common general model of multiple risks assessment, articulated in different stages, can be adopted. It is not possible, however, to apply a single set of criteria in all cases of data processing.

Nevertheless, general standards and criteria can be adopted with regard to different data processing endeavours relating to the same areas (e.g., healthcare, geolocation, direct marketing). This is consistent with a context-based approach (e.g. concepts of necessity and proportionality) and with models based on co-regulation, which have been adopted in the EU and other countries.

Once this multiple-impact assessment is approved by DPAs, the related data processing is considered secure in terms of both protection of personal information and social impact. As a consequence, companies can enlist users in the data processing without any prior consent provided they give notice of the results of the assessment and provide an opt-out option.

This assessment represents an economic burden for companies, but allows those who pass to use data for complex and multiple purposes, without requiring users to opt-in.

From the users' side, the assessment supervised by DPAs provides an effective evaluation of risks, while the option to opt out allows users to choose to not be a part of the data collection.

The suggested model represents a significant change in the traditional approach to data protection. For this reason, it is necessary to provide a subset of rules for big data analytics, focused on a multiple risk assessment, a deeper level of control by DPAs, and the opt-out model.

From the behavioral and cultural perspective, this new approach would have a greater impact on companies and DPAs than consumers.

Consumers will benefit from a more secure environment, while corporations and DPAs will have to invest more resources in risk assessment and acquire specific competence.

This approach will create a safer environment for consumers, particularly as society looks toward a future characterized by the roles played by big data, expert systems, and artificial intelligence. This perspective makes it easier to envision a future scenario in which privacy-oriented and trustworthy services increase a user's propensity to share data and stimulate the digital economy and fair competition.

Additional Reading

Cohen, Julie E. "What Privacy is For," 126 Harv. L. Rev. 1904, (2013).
Dwork, Cynthia, and Deirdre K. Mulligan. "It's not Privacy and It's not Fair," 66 Stan. L. Rev. Online 35 (2013).
Keats Citron, Danielle. "Technological Due Process," 85(6) Wash. U. L. Rev. 1249 (2008).

Mayer-Schönberger, Viktor and Kenneth Cukier. Big Data. A Revolution That Will Transform How We Live, Work and Think (London: John Murray, 2013).

Rubinstein, Ira S. "Big Data: The End of Privacy or a New Beginning?," 3(2) Int'l Data Privacy L. 74 (2013).

Schwartz, Paul M. "Data Protection Law and the Ethical Use of Analytics," CIPL (2010), http://www.huntonfiles.com/files/webupload/CIPL_Ethical_Undperinnings_of_Analytics_Paper.pdf.

Tene, Omer and Jules Polonetsky. "Privacy in the Age of Big Data: A Time for Big Decisions," 64 Stan. L. Rev. Online 63 (2012).

In the Age of the Web, What Does "Public" Mean?

David R. O'Brien

The web is catalyzing a quiet revolution in social science and behavioral research. Researchers are using it as a source of detailed information about humans, and the variety and amount of available data may yield new insights into human behaviors.[1] Users of online services such as Facebook and Twitter generate large amounts of personal information as they create profiles, communicate with others, share video and images, leave comments on blogs, and otherwise interact with the web. Researchers can easily extract this information using automated software tools to build datasets for analysis, increasing the speed at which large data can be complied while simultaneously reducing the managerial burdens. The richness and quantity of the data promises to give researchers the "the capacity to collect and analyze an unprecedented breadth and depth of scale."[2] Despite the provocative insights that may result from this new vein of data, these emerging practices fall into a category of human subjects research in which the legal and ethical standards are unclear. At the heart of the matter are some difficult questions about the boundaries between public and private information.

In the US, certain types of academic research on humans are governed by regulations known as the Common Rule.[3] These regulations are designed to decrease the risk of psychological and physical harm to human subjects by requiring academic institutions to establish Institutional Review Boards (IRBs) and oversight programs to review and approve research studies conducted at their institutions. For example, a researcher might be required to disclose to potential subjects the nature of the study, obtain meaningful consent, and put in place controls to protect the security and confidentiality of any sensitive data collected from subjects.

Not all research on humans is subject to the Common Rule. Studies that only use publicly available information, which potentially includes information mined from the web, have long been an exempt category.[4] The term public, in this sense, is synonymous with benign—if the information was collected from a public source, analyzing and disseminating it is not considered harmful to the person to whom it pertains. More importantly, if a research study falls into this category, institutions are not required to oversee it. The public-private distinction in the Common Rule owes its origins to privacy law, which has traditionally held that public information is not subject to privacy protections.[5]

While the public-private distinction made sense for a world in which the costs of obtaining information were greater, one might question whether it remains sensible. For instance, it does not account for the potential vulnerabilities of users who might become unwilling participants in studies, or the techno-social privacy norms to which communities adhere as they publish and share information online. As evidenced in recent studies, there is a startling disconnect between user expectations of privacy on the Internet and their legal realities.[6] Users may not fully understand or appreciate the consequences of their actions when they decide to publish, only to later regret them without recourse. Normative behaviors around privacy on the web have also been shown to be more nuanced than previously thought. Recent scholarship has illustrated how community norms and the specific contexts in which individuals share information play an important role in shaping user notions of privacy.[7] Although they choose to publish, these users may believe their audience is limited to only those they

target or to a community that will respect normative boundaries. This leaves room for users to feel violated when their information is taken from one context and placed in a new context that they did not anticipate.

On the other hand, the web is often described as a one-to-many or many-to-many medium in which people are interconnected with indistinct boundaries in "networked publics."[8] Most information published to the web is indexed and discoverable through search engines, and it is capable of being copied and stored indefinitely. After publishing to the web, a user effectively relinquishes control, making the information ostensibly public. In many respects, these characteristics lend support to the argument that information on the web should be considered public, regardless of what users expect or intend. Indeed, they are often cited by researchers and IRBs as the basis for why studies that use information mined from the web are currently subject to minimal oversight in practice.[9]

Nevertheless, ethicists and researchers are increasingly flagging the lack of clear ethical guidance as problematic,[10] and changes to the public-private distinction as used in research may be on the horizon. In 2013 the US Department of Health and Human Services, the agency responsible for administering the Common Rule, released draft guidelines that urge researchers to note "expressed norms or requests in a virtual space, which—although not technically binding—still ought to be taken into consideration."[11] A number of associations within the field of social science have also begun crafting new ethical guidelines for data mining practices which, among other things, suggest deliberative decision-making processes to help researchers identify potential risks on a case-by-case basis.[12] While these developments give some clues to the trajectory of new policy and ethics, more research and public debate is needed to better understand the potential risks to users.

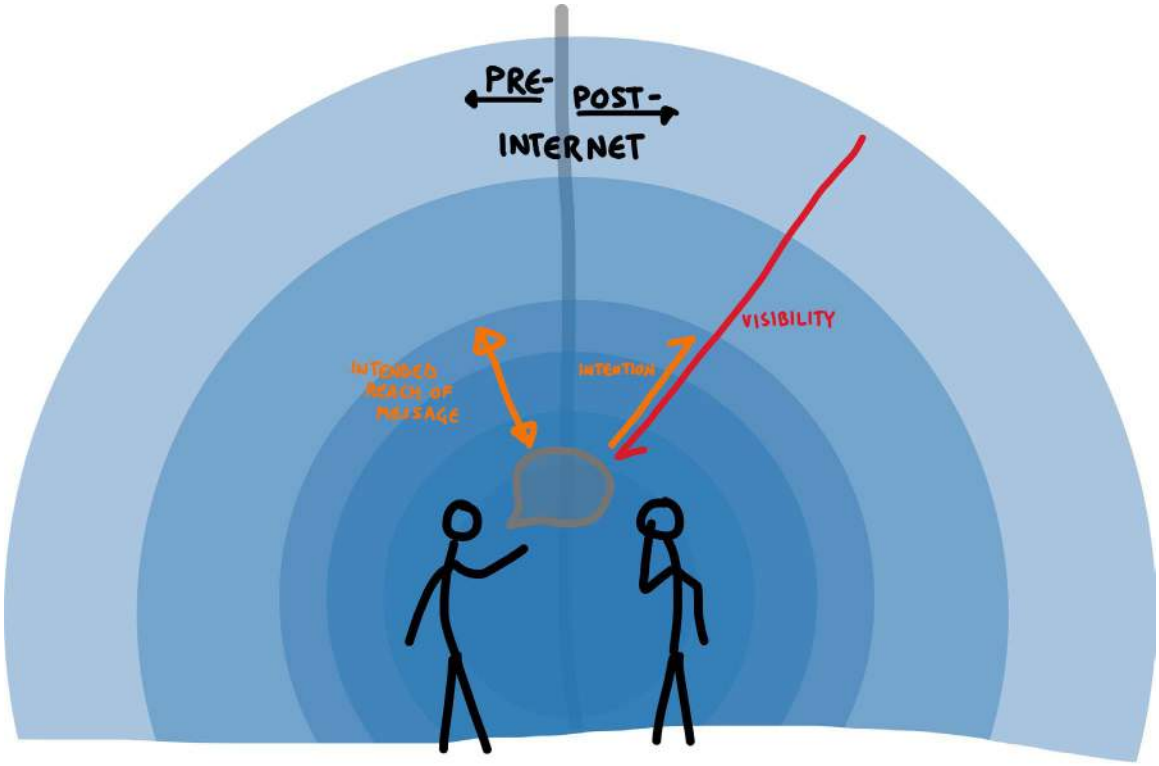


Illustration by Willow Brugh

Notes

1 See Gary King, "The Changing Evidence Base of Social Science Research," in Gary King, Kay Scholzman, Norman Nie, eds., The Future of Political Science: 100 Perspectives (New York: Routledge Press, 2009).
2 David Lazer, et al., "Computation Social Science," Science, vol. 323, issue 5915 (February 6, 2009),: pp.721-723.
3 45 CFR § 46, et seq.
4 45 CFR § 46.102(f) (defining "human subject" as "a living individual about whom an investigator obtains: (1) data through intervention or interaction with the individual, or (2) identifiable private information.") To the extent data mining is possible without interacting with a subject, which is often a trivial matter, and provided the information is not "private," the research is not subject to these regulations.
5 See, e.g., Ryan Calo, "The Boundaries of Privacy Harm," Indiana Law Journal, vol. 86 (Summer 2011): pp.1131-1162; Orin Kerr, "Applying the Fourth Amendment to the Internet: A general approach," Stanford Law Review, vol. 62 (2010), pp. 1027-1036.
6 See, e.g., Mary Madden, "Privacy management on social media sites," Pew Research Internet Project, February 24, 2012, http://www.pewinternet.org/2012/02/24/privacy-management-on-social-media-sites/; Yabing Liu, Krishna P. Gummadi, Balachander Krisnamurthy, Alan Mislove, "Analzying facebook privacy settings: user expectations vs. reality," Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement (2011): pp.61-70; Alessandro Acquisti and Jens Grossklags, "Privacy an Rationality in Individual Decision Making," IEEE Security & Privacy (January/February 2005), pp.24-30.
7 See Helen Nissenbaum, Privacy in Context: Technology, Policy, and the Integrity of Social Life (Stanford: Stanford Law Books, 2010); Leslie K. John, Alessandro Acquisti, and George Lowenstein, "The Best of Strangers: Context Dependent Willingness to Divulge Personal Information Online," Journal of Consumer Research, vol. 35, issue 5 (2011).
8 See danah boyd, "Why youth (heart) social network sites: The role of networked publics in teenage social life," in David Buckingham, ed., MacArthur Foundation Series on Digital Learning – Youth, Identity, and Digital Media Volume (Cambridge: MIT Press, 2007); Yochai Benkler, The Wealth of Networks: How Social Production Transforms Markets and Freedom, (New Haven: Yale University Press, 2006).
9 See Lauren B. Solberg, "Regulating Human Subjects Research in the Information Age: Data mining of social networking sites," Northern Kentucky Law Review, vol. 39 (2012): pp. 327-358.
10 See, e.g., Ilka Gleibs, "Turning Virtual Public Spaces into Laboratories: Thoughts on Conducting Online Field Studies Using Social Network Sites," Analyses of Social Issues and Public Policy, vol. 00, issue 0 (2014): pp. 1-9; Jacquelyn Burkell, "Facebook: public space, or private space," Information Communications & Society, vol. 17, issue 8 (2014): pp. 974-985; R. Benjamin Shapiro and Pilar N. Ossorio, "Regulation of Online Social Network Studies," Science, vol. 339, issue 6116, (January 11, 2013): pp.114-145; Michael Zimmer, "But the data is already public: on the ethics of research in Facebook," Journal of Ethics and Information Technology, vol 12, issue 4 (December 2010).
11 SACHRP, US Dept. of Health and Human Services, "Considerations and Recommendations Concerning Internet Research and Human Subject Research Regulations, with Revisions," March 12, 2013, http://www.hhs.gov/ohrp/sachrp/mtgings/2013%20March%20Mtg/internet_research.pdf.
12 See, e.g., Caitlin Rivers and Bryan Lewis, "Ethical research standards in a world of big data," F1000Research, http://f1000research.com/articles/3-38/v2; Annette Markham and Elizabeth Buchanan, Association of Internet Researchers, "Ethical Decision-Making and Internet Research: Recommendations from the AOIR Ethics Committee," August 2012, http://aoir.org/reports/ethics2.pdf.

Code is Law, But Law is Increasingly Determining the Ethics of Code

Jonathon W. Penney

In late July 2014, the information security world was on edge. Researchers from Carnegie Mellon University—who work "closely with the (US) Department of Homeland Security"—were scheduled to give a talk at the Black Hat USA infosec conference on a simple method to "de-anonymize" Tor users.[1] Many were skeptical. Tor, after all, was a respected and widely used tool for online anonymity, employed by activists, dissidents, journalists, and yes, criminals too, to cloak their activities from the prying eyes of state authorities at home and abroad; even Edward Snowden trusted its protection.[2] The idea that there was an undisclosed vulnerability that could be exploited "on a budget" to cheaply and easily unveil the identity of Tor users,[3] was difficult to believe. And yet, the security researchers in question, from the CERT unit of the CMU Software Engineering Institute (SEI), seemed credible.[4] So, people withheld judgment and waited for the talk.

But the talk never happened. It was pulled from the conference program at the last minute, with the CMU researchers, as reported in The Washington Post, claiming the materials they planned to present had "not yet been approved by CMU/SEI for public release".[5] There was plenty speculation as to the reason for the cancellation, with some suggesting a possible National Security Letter from a federal agency,[6] while others argued CMU lawyers, likely concerned by the legality of some aspects of the research, killed the talk to avoid potential liabilities.[7] The cancellation also led commentators to raise important ethical questions about the CMU research—had users' privacy been violated or laws broken? Were identities of Tor users harvested without their consent? Was CMU's Institutional Review Board—the body responsible for overseeing ethical approval for research—properly consulted? None of these questions have yet been fully debated or answered, and may not ever be. All that we can say for sure, is that the cancellation notice sent to the Black Hat USA conference came from CMU's legal counsel.[8] The law had foreclosed any ethics debate. It wasn't always like this.

Perhaps the most contentious ethics debate in the infosec community took place in the late 1990s and early 2000s, and occurred beyond, and sometimes in spite of, any relevant law. That debate was prompted by the Anti-Sec Movement and concerned the ethics of "full disclosure"; that is, the infosec industry practice—the industry norm at the time—to fully disclose security vulnerabilities in various online security forums, justified as the best means to force, or shame, vendors into patching those security holes.[9] Full disclosure itself was a product of "frustration" with an earlier and much criticized Computer Emergency Response Team (CERT) based disclosure process, wherein "bugs" were reported to CERT but kept secret until patched, with venders often dragging their feet or simply not bothering patching at all.[10] Full disclosure, so the argument went, created public pressure to encourage venders to patch vulnerabilities and do so quickly.

The hackers in the anti-sec movement disagree. They strongly opposed full disclosure, and targeted high profile infosec industry figures aligned with such disclosure practices—like OpenBSD's Theo de Raadt or Aleph1 of SecurityFocus—with hacks to make their point. Now, to be clear, anti-sec, particularly its more "violent incarnations"[11] like Pr0j3kt M4yh3m and Phrack High Council, was prone to trolling and exaggeration, and often unnecessarily offensive, but at bottom there remained an im-

portant ethos to the anti-sec movement: it took aim at the commercialization and greed it believed was overtaking the infosec community,[12] and they were not alone as many in the broader community agreed with that sentiment.[13] Full disclosure, anti-sec advocates believed, had nothing to do with security and everything to do with certain infosec practitioners building their public profile via publishing bugs and exploits to curry favor with corporate interests and secure lucrative security jobs.[14] For anti-sec, full disclosure was not only betrayal of the hacker underground, but also deeply irresponsible security wise—because even with public disclosure venders were still slow to patch, leaving any "script kiddie" with an Internet connection to wreak havoc with published exploit code.[15]

Whatever your views on their modus operandi, the antisec movement did provoke a broader debate over security vulnerability disclosure practices, with far ranging implications. Disclosure practices ultimately evolved with "responsible disclosure" now the norm, where researchers work behind the scenes with vendors to protect end users, but usually with a fixed deadline for publication to incentivize bug fixing.[16] Applied properly, it balances incentives for vendors to act, while avoiding the problems with what Bruce Schneier calls "bug secrecy" (personified by the CERT reporting system) and the dubious ethical practice (and broader insecurities) resulting from full vulnerability disclosure that anti-sec movement criticized.[17] Here, abroad and contentious debate within a research community led to better ethics and security practices in the wider industry.

But plenty has changed since the days of Pr0j3kt M4yh3m; most importantly, the legal landscape. Expansive laws like the Computer Fraud and Abuse Act (CFAA) and the Digital Millennium Copyright Act, coupled with aggressive enforcement by state authorities and corporate interests, have subjected an increasing array of online activities to criminal and civil penalty. What was once considered "full disclosure" may today constitute a criminal act under the CFAA or DMCA.[18] The Tor de-anonymization talk, which may have once led to a much needed infosec community debate about research ethics and the security and dignity of users, was cut off by lawyers and legal concerns. Similar problems are arising in data research beyond information security. The discussion concerning the controversial Facebook "contagion" study, for example, was arguably also dominated by lawyers, with concerns about the study's legality potentially deterring similar research or, at least, publication thereof, in the future.[19] A "destructive silence" from social computing researchers and data scientists on the broader social, technological, and ethical implications of the Facebook study was filled by the lawyers and legal questions.[20]

"Code is Law", the aphorism Larry Lessig popularized, spoke to the importance of computer code as a central regulating force in the Internet age. That remains true, but today, overreaching laws are also increasingly subjugating important social and ethics questions raised by code to the domain of law. Those laws—like the CFAA and DMCA—need to be curtailed or their zealous enforcement reigned; they deter not only legitimate research but also important related social and ethics questions. But researchers must act too. The infosec community, and research communities like it, must not fall silent in the face of legal threats nor tolerate research censorship, as is the case with the Tor de-anonymization talk. The point is not that researchers must launch some divisive "project" or movement within this or that discipline; only that they need, at the very least, to re-assert control over the social, legal, and ethical direction of their fields. Otherwise, law will increasingly determine the direction of data science and the ethics of code.

Notes

1 Andrea Peterson, "Why was the Black Hat Talk on Tor de-anonymization mysteriously cancelled?," The Washington Post, July 24, 2014, http://www.washingtonpost.com/blogs/the-switch/wp/2014/07/24/why-was-the-black-hat-talk-on-tor-de-anonymization-mysteriously-canceled/.
2 Gerry Smith, "Meet Tor, The Military Made Privacy Network That Counts Edward Snowden as a Fan," The Huffington Post, August 8, 2013, http://www.huffingtonpost.com/2013/07/18/tor-snowden_n_3610370.html.
3 Peterson, ibid.
4 Peterson, ibid.
5 Peterson, ibid.
6 Richard Byrne Reilly, "How (and Why) feds killed a talk on Tor hacking at Black Hat," Venturebeat News, August 6, 2014, http://venturebeat.com/2014/08/06/how-why-feds-killed-a-talk-on-tor-hacking-at-black-hat-exclusive/.
7 Peterson, ibid.
8 Ionut Ilascu, "TOR Talk at Black Hat USA 2014 Cancelled," Softpedia, July 22, 2014, http://news.softpedia.com/news/TOR-Talk-at-Black-Hat-USA-2014-Cancelled-451645.shtml.
9 Bruce Schneier, "Full Disclosure," Crypto-Gram Newsletter, November 21, 2001, https://www.schneier.com/crypto-gram-0111.html.
10 Schneier, ibid.
11 Brian McWilliams, "White Hat Hate Crimes On The Rise," Wired, August 13, 2002, http://archive.wired.com/culture/lifestyle/news/2002/08/54400?currentPage=all.
12 Kim Zetter, "Coder Journeys From Wall Street to Prison," Wired, May 7, 2010, http://www.wired.com/2010/05/watt-reports-to-prison/all/. ("...Project Mayhem's "anti-sec" stance wasn't completely unwelcome in the security world. There was a sentiment among some in the DefCon crowd that the security community's focus on profit was at odds with hacking's roots..."); Schneier, ibid. ("...Publishing a security vulnerability is often a publicity play; the researcher is looking to get his own name in the newspaper by successfully bagging his prey...").
13 AntiSecurity, Intro/Manifesto, ibid. Phrack Inc., ibid; Zetter, ibid.
14 AntiSecurity, Intro/Manifesto, ibid. Phrack Inc., ibid. Zetter, ibid.
15 AntiSecurity, Intro/Manifesto, ibid.; Schneier, ibid. ("...Handing attack tools to clueless teenagers is part of the problem..."); Phrack Inc., ibid.
16 Chris Evans, Eric Grosse, Neel Mehta, Matt Moore, Tavis Ormandy, Julien Tinnes, Michel Zalewski (Google Security Team), "Rebooting Responsible Disclosure: A focus on protecting end users," Google Online Security Blog, July 20, 2010, http://googleonlinesecurity.blogspot.co.uk/2010/07/rebooting-responsible-disclosure-focus.html; Schneier, ibid.
17 Evans et al., ibid; Schneier, ibid.
18 Mike Masnick, "The DOJ's Insane Argument Against Weev: He's a Felon Because He Broke The Rules We Made Up," Techdirt, September 30, 2013, https://www.techdirt.com/articles/20130929/15371724695/dojs-insane-argument-against-weev-hes-felon-because-he-broke-rules-we-made-up.shtml; Schneier, ibid. (discussing controversy over Niels Ferguson's Linux vulnerability discovery and the DMCA).
19 Jonathan Zittrain, "Facebook Could Decide an Election Without Anyone Ever Finding Out," The New Republic, July 1, 2014, http://www.newrepublic.com/article/117878/information-fiduciary-solution-facebook-digital-gerrymandering (speaking of new laws imposed on intermediaries like Facebook for their internal studies as "ill advised"); Robinson Meyer, "Facebook's Mood Manipulation Experiment Might Have Been Illegal," The Atlantic, September 24, 2014, http://www.theatlantic.com/technology/archive/2014/09/facebooks-mood-manipulation-experiment-might-be-illegal/380717/; Mike Masnick, "Law Professor Claims Any Internet Company 'Research' On Users Without Review Board Approval Is Illegal," Techdirt, September 24, 2014, https://www.techdirt.com/articles/20140924/00230628612/law-professor-claims-any-internet-company-research-users-without-review-board-approval-is-illegal.shtml.
20 Michael Bernstein, "The Destructive Silence of Social Computing Researchers," Medium, July 7., 2014, https://medium.com/@msbernst/the-destructive-silence-of-social-computing-researchers-9155cdff659; Lorenzo Franceschi-Bicchierai, "Facebook Playing Your Feelings Is Legal But 'Creepy' Say Law Experts," Mashable, July 1, 2014, mashable.com/2014/07/01/facebook-emotions-study-legal/.

Dada Data and the Internet of Paternalistic Things

Sara M. Watson

This contribution is speculative fiction about a possible data-driven future.

My stupid refrigerator thinks I'm pregnant.

I reached for my favorite IPA, but the refrigerator wouldn't let me take one from the biometrically authenticated alcohol bin.

Our latest auto-delivery from peaPod included pickles, orange juice, and prenatal vitamins. We never have orange juice in the house before because I find it too acidic. What machine-learning magic produced this produce?

And I noticed the other day that my water target had changed on my Vessyl, and I wasn't sure why. I figured I must have just been particularly dehydrated.

I guess I should have seen it coming. Our Fountain™ tracking toilet noticed when I got off hormonal birth control and got an IUD instead. But I thought our toilet data was only shared between Nest and our doctors? What tipped off our Samsung fridge?

I got a Now notification that I was ovulating a few weeks ago. I didn't even know it had been tracking my cycle, let alone by basal body temperature through my wearable iRing. I certainly hadn't turned that feature on. We're not even trying to have a baby right now. Or maybe my Aria scale picked up on some subtle change in my body fat?

Or maybe it was ComWarner? All our appliances are hooked up through one @HomeHub. I didn't think twice about it because it just worked—every time we upgraded the dishwasher, the thermostat. Could it be that the @HomeHub is sharing data between the toilet and our refrigerator?

I went into our @HomeHub interface. It showed a bunch of usage graphs (we've been watching a "below average" amount of TV lately), but I couldn't find anything that looked like a pregnancy notification. Where was this bogus conception data coming from?

My iWatch pinged me. The lights in the room dimmed, and a connected aromatherapy candle lit up. The heart monitor on my bra alerted me that my heart rate and breathing was irregular, and that I should stop for some meditative breathing. I sat down on my posture-tracking floor pillow, and tried to sink in.

But I couldn't keep my mind from wandering. Was it something in the water? Something in my Snap-Texts with Kathryn? If it was true, why hadn't my doctor called yet? Could I actually be pregnant?

I turned on the TVTab to distract me, but I was bombarded with sponsored ads for "What to Expect When You're Expecting 9.0" and domain squatter sites that search for a unique baby name.

I searched for similar incidents on the Quorums: "pregnancy Samsung refrigerator," "pregnancy Fountain toilet." Nothing. I really wanted to talk to someone, but I couldn't call Google because they don't have customer service for @HomeHub products. I tried ComWarner. After waiting for 37 minutes to speak with a representative, I was told that the he couldn't give out any personal data correlations over the phone. What bureaucratic bullshit!

It can't be true. Russell has been away in Addis Ababa on business for the three weeks. And I've still got the IUD. We aren't even trying yet. This would have to be a bio-correlative immaculate conception.

I tapped Russell on his iWatch three times, our signal to call me when he is done with his meeting. I was freaking out.

I could have really used that beer. But the fridge still wouldn't let me take it. What if I am really pregnant? I opened up Taskr to see if could get an old fashioned birth control test delivered, but price was three times as expensive as it normally would be. I considered CVS, but I thought better of it since you can't go in there anymore without a loyalty card. It was far, but I skipped the self-driving Uber shuttle and walked the extra mile to the place that accepts crypto, where I wouldn't be tracked. I think. And that's when I got the notification that my funding interview for my new project the following morning had been canceled.

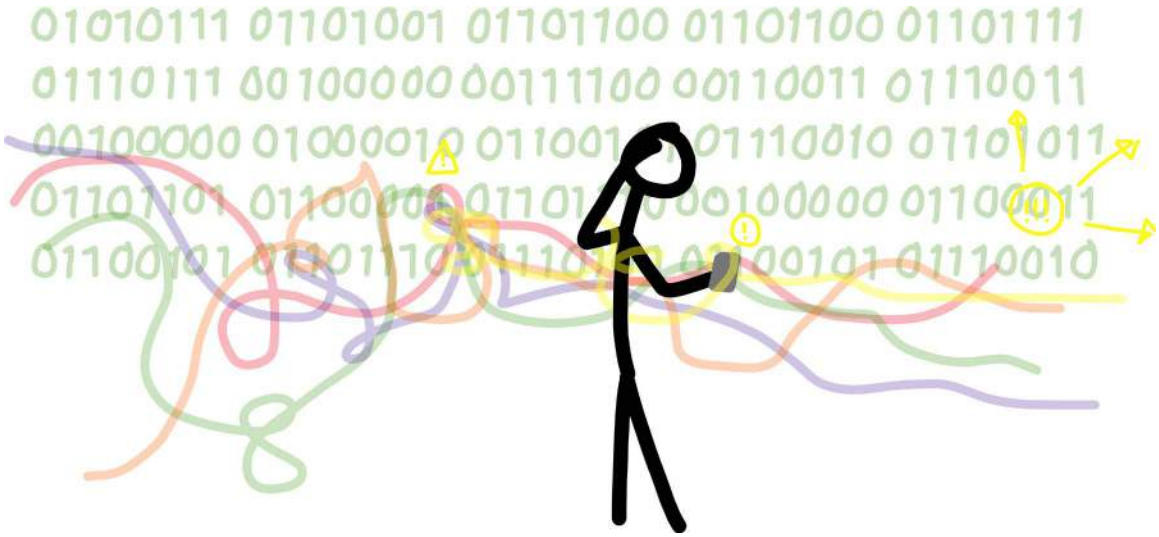
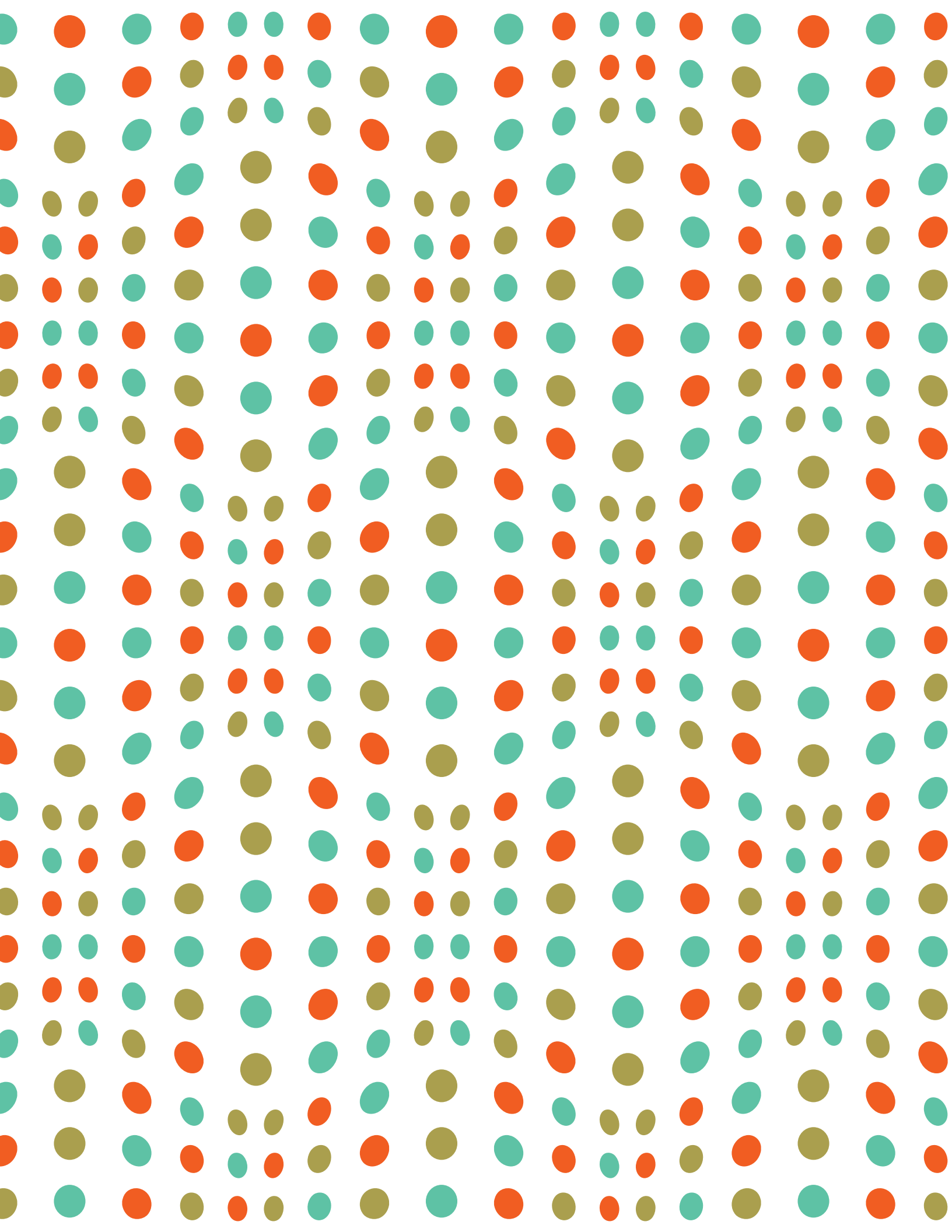


Illustration by Willow Brugh



PUBLIC DISCOURSE

Robert Faris

The examples of civil society using digital communication tools to influence public discourse and engage in collective action around the globe are piling up; there are plentiful signs of changing power dynamics in many corners of the world. Yet the debate over the salutary influence of the Internet on public discourse, democracy, and government is far from settled. Many of the transformational changes promised by some have not come to pass. Moreover, some groups use the Internet in a diametrically opposite direction: exploiting the Internet to suppress the initiatives of those working to promote democratic reforms and protect civil liberties.

The potential of digital communication platforms as a tool for helping to organize protests and social movements has been demonstrated repeatedly, from some of the earliest color revolutions of the Philippines, Myanmar, Ukraine, and Iran through the Arab spring and Occupy to several large social movements of 2014. Taiwan's Sunflower movement, which took place in early 2014, is a prime example. The adept use of digital tools by protest organizers helped them to quickly scale up protests to over 100,000 participants.[1] The Euromaidan protests in Ukraine that led to change of government in early 2014 were heavily influenced by social media organizing and informed by the social mobilization strategies of the Orange Revolution of 2004-2005. Beyond just letting people know that protests are taking place, recent research during the Euromaidan protests indicates that social networks, both online and off, seem to be important in getting people onto the streets for the first protest events, which are often the most risky in more authoritarian countries. We also see evidence that messages that go viral online subsequently show up as signage at offline protests, impacting how movements frame their messages as well as the claims against them.[2]

In Hong Kong, the Occupy Central protests included a large number of technologically literate young people using a variety of platforms, including Facebook, Twitter, Instagram, WhatsApp, and WeChat, to successfully organize and sustain the protest movement over many weeks. The downside of employing open communication strategies are well known; digital communication is subject in varying degrees to surveillance, blocking, and misinformation campaigns. During the Occupy Central protests, it was reported that some protestors received text messages inviting them to download an app that contained malware used for surveillance. One messaging app, Telegram, as well as a number of prominent pro-democracy sites, were taken down by massive DDoS attacks. FireChat, an app that enables mesh networking, became a popular choice for protestors. This allowed users to communicate directly to one another without routing messages through overloaded cell towers. It is well established that digital tools are helpful in coordinating protests and revealing popular sentiments. This represents a clear threat to unpopular governments and offers a strong avenue for opposing unpopular policies that capture the public attention.

We've long recognized that the links between new media and social mobilization do not translate easily into improving governance or the nuts and bolts of policymaking, even after bringing tens of thousands of protestors into the streets and toppling governments. The organizational challenges of sustaining political coalitions through elections and cycles of government are fundamentally different

from inspiring mass protests, and it is unclear that the structures and coalitions that emerge for and from such protests are suited for that task. While there are a growing number of specific examples in which civil society voices that are aggregated and amplified through the networked public sphere have had an impact on policy decisions, it is not clear that there exist mechanisms and transition paths toward empowering existing or new organizations that are able to leverage disperse networks in similar ways across many topics in a sustained way. An interesting case to watch in the future is the Podemos Party in Spain that evolved out of the 15M movement of 2011-12.

The networked public sphere can be effective in rallying like-minded individuals around matters of common concern. In addition to countering inaccurate 'official' versions of events, networked communication can address some of the coordination problems associated with collective action to overcome the classic articulation of the problem by Mancur Olson: that smaller well-coordinated interest groups are able to use the political process to serve their own interests because of the failure of the broader public to organize their opposition.[3] Several examples—the massive influx of public comments to the FCC in support of net neutrality in the United States[4] and the mass protests against Mexico's proposed telecommunications bill[5] are two—show promise for broad-scale coordination to overcome issues of collective action, while a number of other issues still appear to be a reach too far, such as climate change and campaign finance reform. It may be that these issues are simply too complex and too polarized, or that they have been simmering in the background of public debate for so long and lack an inciting event to serve as a spark that pushes people to react to them online.

Much hope has been placed in the Internet to shine light upon government mismanagement, corruption, and abuse and to thereby act as an impetus and mechanism for better governance.
In places where media is tightly controlled by the government or highly concentrated media dominates news coverage, alternative media has proven capable of introducing issues into the public agenda and offering alternative frames. Some of the promise of using new media to increase transparency in government and matters of public import has been realized. Video shot by citizens continues to offer a powerful means for holding those in power accountable for their actions. In the United States, video accounts of police using force in arresting citizens have helped to propel and sustain debates over racial injustice and the excessive use of force by police. In Turkey, citizen video of the Gezi Park protests helped fill a void left by mainstream media outlets, most of which either supported the ruling party or self-censored for fear of government retribution. In Tunisia, marsad.tn was established as a local elections and parliamentary action monitoring group designed to increase transparency and more accountability in politics. However, it is still far from clear whether digital transparency might significantly and broadly improve governance.[6]

Social media and digital communication have brought attention to events and issues to a larger public and sustained public debates that might not have otherwise risen to such prominence in the public agenda. Debates over race and gender equality are an ongoing phenomenon in many countries around the globe, frequently transcending their more narrow locally-rooted and event-based origins. The deaths of Michael Brown in Ferguson, Missouri and Eric Gardner in New York City have sparked both demonstrations and deep discussions of race across the United States,[7] while the assault of two young women on a bus in Rohtak, India—which recalled the 2012 fatal gang rape of another young

woman on a bus in Delhi in 2012— has fueled a national dialogue on gender equality in the country.[8] One explanation for this is that online discussions are open for greater participation, amplification, and scrutiny compared to conversations in the past that would have been restricted to a smaller community of like-minded individuals. In discussions among groups that never would have crossed paths before, we see examples that range from high-minded discourse to acrimonious debate, vitriol, and threats of violence, and we see examples of local conflict being elevated to a broader public stage. A possible explanation for this phenomenon is that the Internet helps with the creation of weak links, and makes them more visible and easier to activate than in the past, thus tying together disparate groups around controversies when they erupt, groups that would not otherwise have been connected. It is still unclear when and where this is helpful, and when it only serves to fan the flames of discord and incite violence.

We still know relatively little about the impact of the networked public sphere in fostering constructive dialogue and compromise across partisan lines, and whether online coverage and debates contribute meaningfully to better understanding complex public issues and crafting solutions. The early indications are that partisanship is alive and well, and that the cognitive biases that inhibit open-minded reconsideration of well entrenched opinions have survived the digital revolution intact. The Gamergate controversy, ostensibly intended to address ethical issues in video game journalism, quickly spiraled into a bitter debate about feminism, misogyny, online harassment, and media conspiracy that was both intensely polarized and highly politicized.[9]

In some places, online communities are taking it upon themselves to address the less constructive variants of online speech. A campaign called Panzagar, organized largely through Facebook, is attempting to combat religiously motivated hate speech in Myanmar by distributing pamphlets, stickers, and flowers.[10] In August, a group of Reddit users posted a public letter to the site's leadership, calling out the site's inaction in response to "barrages" of "hateful, racist" posts and sparking a broad discussion of hate speech in the online community, which has over 170 million members.[11] Online volunteer-based initiatives to end violence against vulnerable segments of society continue to emerge. One example is HarassMap, which aims to end the social acceptability of sexual harassment and assault in Egypt. It is still unclear to what extend such initiatives can influence public attitudes and government policies.

One thing that is clear is that social media leaves everything out there to see, forcing us to recognize issues that might have otherwise been obscured. An optimistic perspective would be that this serves as a fire alarm for underlying issues that require attention and that hostile interactions on social media compel us to find solutions. A less sanguine assessment is that the open expression of such acrimony only serves to incite and fuel deeper societal schisms.

Notes

1 Michael Gold and James Pomfret, "Over 100,000 protest in Taiwan over China trade deal," Reuters, March 30, 2014, http://www.reuters.com/article/2014/03/30/us-taiwan-protests-idUSBREA2T07H20140330.

2 Olga Onuch, Social Networks and Social Media in Ukrainian 'Euromaidan' Protests, January 2, 2014, http://www.washingtonpost.com/blogs/monkey-cage/wp/2014/01/02/social-networks-and-social-media-in-ukrainian-euromaidan-protests-2/.

3 Mancur Olson, The Logic of Collective Action: Public Goods and the Theory of Groups (Cambridge: Harvard University

Press, 1971).

4 Jacob Kastrenakes, "FCC received a total of 3.7 million comments on net neutrality," The Verge, September 16, 2014, http://www.theverge.com/2014/9/16/6257887/fcc-net-neutrality-3-7-million-comments-made.

5 Juan Montes, "Social Media Protests in Mexico Shape Telecom Bill," The Wall Street Journal, April 23, 2014, http://www.wsj.com/articles/SB10001424052702304788404579519633220313644.

6 David Frum, "The Transparency Trap," The Atlantic, August 13, 2014, http://www.theatlantic.com/magazine/archive/2014/09/the-transparency-trap/375074/.

7 Nancy Scola, "Watch as Twitter shifts from "#BlackLivesMatter" to "#ICantBreathe"—and back again," Washington Post, December 5, 2014, http://www.washingtonpost.com/blogs/the-switch/wp/2014/12/05/watch-as-twitter-shifts-from-blacklivesmatter-to-icantbreathe-and-back-again/.

8 Nikhil Dhingra, "India's 'Braveheart' Sisters Fight Back Against Sexual Predators," Global Voices Online, December 3, 2014, http://globalvoicesonline.org/2014/12/03/indias-braveheart-sisters-fight-back-against-sexual-predators/.

9 Ezra Klein, "Gamergate and the politicization of absolutely everything," Vox, November 1, 2014, http://www.vox.com/2014/11/1/7136343/gamergate-and-the-politicization-of-absolutely-everything. See also Andy Baio, "72 Hours of #Gamergate," Medium, October 27, 2014, https://medium.com/message/72-hours-of-gamergate-e00513f7cf5d.

10 Hereward Holland, "Facebook in Myanmar: Amplifying hate speech?," Al Jazeera, June 14, 2014, http://www.aljazeera.com/indepth/features/2014/06/facebook-myanmar-rohingya-amplifying-hate-speech-201461211283429014 4.html.

11 Jason Abbruzzese, "Hate Speech Is Drowning Reddit and No One Can Stop It," Mashable, October 26, 2014, http://mashable.com/2014/10/26/reddit-hate-speech-moderation/.

Flower Speech: New Responses to Hatred Online

Susan Benesch

From threats to rape the children of an online game developer,[1] to a dustpan full of ashes labeled "one good Jew"[2] or a hashtag meaning "let's burn gays,"[3] hatred online often seems uncontrollable—except with censorship that would also curb freedom of expression. Possibly not, though: tech activists are testing new methods to counter digital vitriol and to protect its targets, employing innovative code, memes, and group efforts.

If successful, this might present an alternative to leaving speech regulation to governments and companies, whose relevant laws and rules are often inconsistent, misapplied, and opaque.

In Myanmar, a new anti-hatred movement called Panzagar or 'flower speech' began in response to hateful and dangerous speech in public and private discourse.[4] Much of this speech describes Muslims as an existential threat to Myanmar as a Buddhist nation. Gruesome images of violence with the tagline "this is what Muslims do" appeared on well-known Facebook pages, implying that Buddhists face a mortal threat. Other cases could hardly be more brazen or explicit: one Facebook account was named "We Will Genocide All the Muslims and Feed Them to the Dogs," in the Myanmar language. (After repeated complaints to Facebook that this violated the company's real-name policy, that account was taken down.)

Panzagar was created in April 2014 by a group of tech activists led by Nay Phone Latt, an Internet café owner, activist, and poet who was sentenced to 20 years in prison in 2008 for violating Myanmar's Electronics Act by reporting news that might tarnish the government's reputation: he had blogged about anti-government protests.[5] He was released in 2012 and is now campaigning against hateful speech and "dangerous speech," a term that I coined[6] for speech that tends to catalyze violence by pitting one group of people against another.

Panzagar began by creating a meme. A person (usually a cute young woman, as drawn by the team's animé-loving volunteer illustrators) holds a flower in her mouth. Taking a cue from this symbolic commitment not to use or tolerate speech that can "spread hate among people," as Nay Phone Latt puts it, thousands of people 'liked' Panzagar's Facebook page within days of its creation, and many have posted photographs of themselves holding flowers in their mouths.[7] This is a courageous act in a country where anti-Muslim feeling is growing and there have been fatal clashes—most recently in July 2014 in Mandalay, after a false rumor that a Buddhist woman had been raped by Muslim men surfaced online and went viral on Facebook.

Facebook so dominates online life in Myanmar that some of its users believe Facebook is the Internet, and have not heard of Google. Many users, however, cannot easily read English, the language of the platform, and are unaware of the 'community standards' or the opportunity to report content. Facebook, for its part, couldn't make much sense of the reports that it received until it hired a Myanmar-speaking subcontractor last year.[8]

Panzagar isn't waiting for Facebook, though. "We need to moderate ourselves without control by others," Nay Phone Latt says. "Both restrictive laws and [hateful] speech are dangers to freedom."[9]

Across the world a few months later, a group of women also argued that violent, hateful content can impinge on freedom of expression. In August 2014, the editors of Jezebel, an American blog directed at women, publicly demanded freedom to write without seeing gifs of rape and other violence against women.

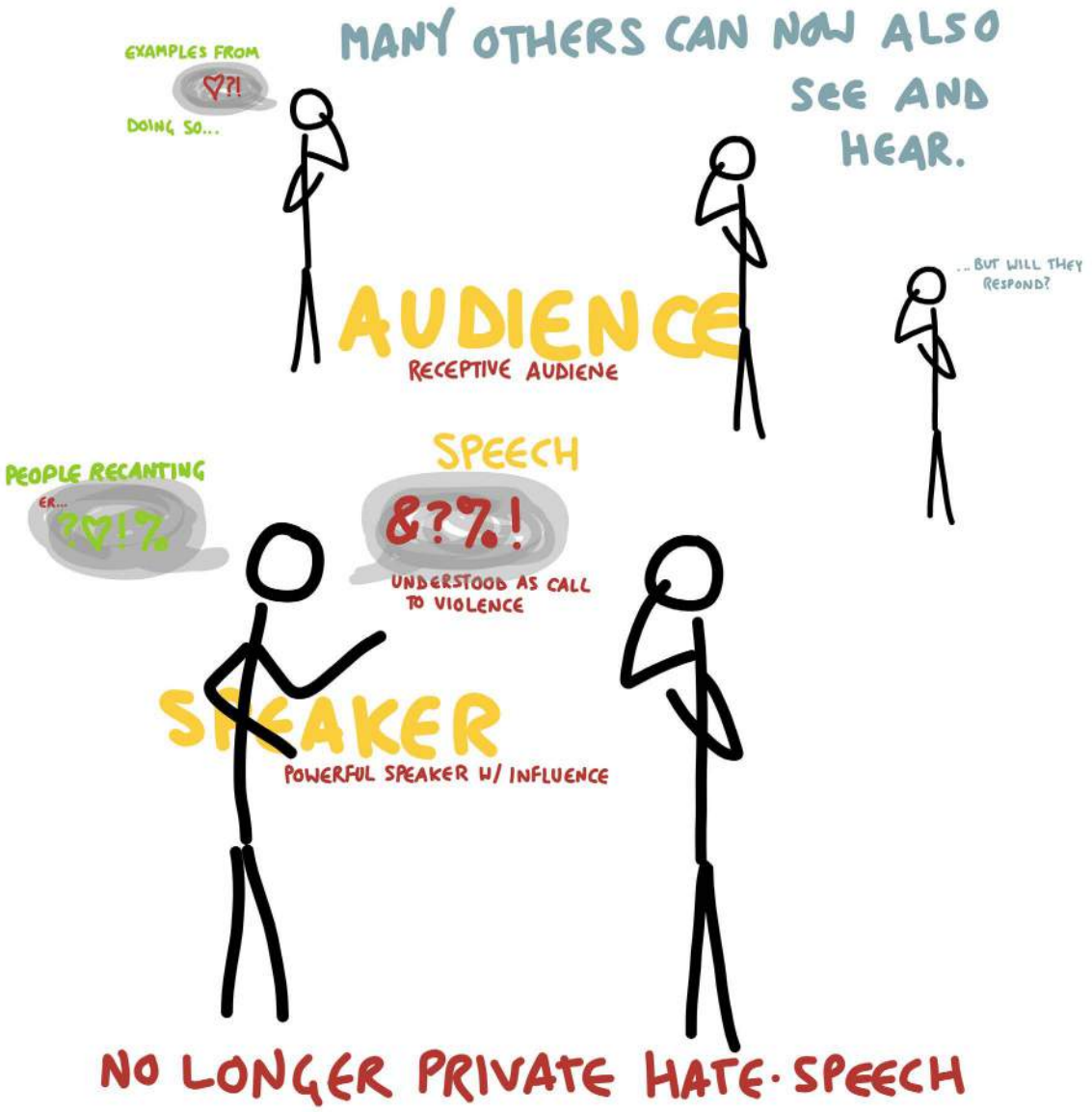


Illustration by Willow Brugh

"It's like playing whack-a-mole with a sociopathic Hydra," they wrote of their efforts to delete gifs that appeared relentlessly on their site, posted as anonymous comments.[10] For months Jezebel readers saw the images, and staffers deleted them manually since their platform, Kinja, provided no alternative. In August, Jezebel editors took the unusual step of posting a public letter to the management of their parent company, Gawker Media. In that brief but impassioned text, the editors demanded a

solution, concluding with an argument that is gaining currency even in the intensely speech-protective land of the First Amendment: some forms of expression constrain the freedom of speech of those who hear or see it, by frightening or even silencing them.[11]

"Gawker has always been a place that would really go to the mat for its writers, a place that offered unmatched freedom to smart people with something to say. It's time that Gawker Media applied that principle to promoting our freedom to write without being bombarded by porn and gore," the editors wrote. The next day, Gawker editorial director Joel Johnson apologized.[12] He later announced that Gawker was disabling image uploads in comments as a temporary fix, and would re-introduce moderation. (Commenters can still remain anonymous.)

Also in response to violent misogyny, this time on Facebook, three activists tried another new tactic. Instead of encouraging supporters to complain to Facebook, Soraya Chemaly, Laura Bates, and Jaclyn Friedman asked supporters to tweet their outrage directly to Facebook advertisers whose ads were sometimes popping up alongside photographs of battered women on pages celebrating domestic violence. Within days, Nissan UK announced that it would pull ads from Facebook, followed by several other companies.

Almost immediately, Facebook said it had failed to remove hate speech, especially gender-based hate, and would "do better."[13] Since then, Facebook has stopped identifying misogynist jokes as "controversial humor" according to Chemaly, and casts a more critical eye on such content.

Taking hateful posts or images off a single platform cannot protect anyone from being personally targeted with threats, doxxing, and fearsome language and images, however, and this tactic has been rampant in the past year. Well-known cases include Zelda Williams, who received tweets with images made to look like the body of her father Robin Williams, soon after he committed suicide; female game developers and critics such as Brianna Wu, Zoe Quinn, and Anita Sarkeesian; and British feminist Caroline Criado-Perez, who was threatened with rape after she campaigned to get women (other than the Queen) featured on UK banknotes. These are, unfortunately, the tip of a grim iceberg.

In response, Hollaback, a nonprofit that works against harassment of women on the street, also wants to "reclaim the streets of the Internet," as its director Emily May puts it. Hollaback is developing a platform that would encourage online 'bystanders' to support people who are being targeted, since this technique has been quite effective offline. It could work even better online, if for no other reason than that bystanders are always available. Millions of them. "With street harassment," May said, "maybe half the time there's somebody else around. The difference is that online, 100% of the time there's somebody else around. It's a public space."

Early data from other contexts suggests that online bystanders can indeed shift discourse norms away from hateful speech, especially in virtual public spaces. In Kenya in 2013, for months before a fraught presidential election, iHub Research (a tech company associated with crowdsourcing pioneer Ushahidi) monitored Kenyan online speech for hateful and dangerous remarks.[14] Such speech abounded, especially in newspaper comment sections and on Facebook.

Among KOT (Kenyans on Twitter), however, there was dramatically less hateful and violent speech.

Trying to understand the great discrepancy, iHub's monitors noticed spontaneous speech regulation on Twitter. In response to hateful Tweets directed at members of particular ethnic groups, other users responded with Tweets such as "please remember that we are all Kenyan" or "Is this the Kenya that we want?" At least one of the original accounts produced an apology, others stopped Tweeting hatred, and some disappeared entirely.

Twitter data from other environments also suggests that "counterspeech" may sometimes convince the authors of hateful speech to change their tune. Nina Davuluri's selection as Miss America 2014 was met with a storm of furious tweets from Americans who confused the daughter of Indian immigrants with an Arab, which made her a presumptive terrorist to some (others were enraged by her skin tone and refused to recognize her as a "real" American).[15]

In one (typically ungrammatical) tweet, a teenaged boy said, "I am literarily soo mad right now a ARAB won #Miss America." He received replies telling him that he was wrong and that his tweet was racist. At first he refused to engage with his new interlocutors, but he eventually tweeted at Davuluri directly, apologizing.

University of Illinois chancellor Phyllis Wise became another target as soon as she decided not to declare a snow day in spite of a very cold weather forecast for Monday, January 27, 2014. Students used the hashtag #fuckphyllis to pelt Wise with racist, sexist, violent threats.[16] Those messages were quickly met with another surge of messages, rebuking those students and defending Wise. The latter messages were more numerous, and may have been more influential.[17]

Influence isn't the same as changing minds or behavior, and counterspeech cannot be expected to shift the minds or behavior of hardcore racists, misogynists, and other haters. Producers of online hatred are not all the same, however—just as members of the groups they target also differ from one another. It may be possible to shift the attitudes of young people, in particular.

Humor is one more tool that is in frequent, and perhaps sometimes effective, use against online hatred. After a UCLA student named Alexandra Wallace recorded herself ranting against Asian students,[18] others posted parodies and responses[19] that were viewed much more than Wallace's clip—in the case of actor Jimmy Wong's "Ching Chong! Asians in the Library Song," more than five million times.[20]

In another case, equally crude racism was met with gentle humor. In response to racist soccer fans' practice of throwing bananas at black players, FC Barcelona's Dani Alves picked up a banana and took a bite during a match in April 2014. Many of his fellow players and fans posted photos of themselves eating bananas, using the hashtag #SomosTodosMacacos ("we are all monkeys").[21] It bears studying whether this changed the minds of any racist monkeys.

Notes

1 Brianna Wu, "Rape and death threats are terrorizing female gamers. Why haven't men in tech spoken out?," The Washington Post, October 20, 2014, http://www.washingtonpost.com/posteverything/wp/2014/10/20/rape-and-death-threats-are-terrorizing-female-gamers-why-havent-men-in-tech-spoken-out/.

2 "#UnBonJuif: Anti-Semitic Hashtag Causes Outrage In France," The Huffington Post, October 16, 2012, http://www.huffingtonpost.com/2012/10/16/unbonjuif-twitter_n_1971676.html.

3 "L'Homophobie sur les réseaux sociaux," Za-Gay, June 3, 2014, http://www.za-gay.org/forum/viewtopic/44740/l-

homophobie-sur-les-reseaux-sociaux/0/.

4 Panzagar, https://www.facebook.com/panzagar. See also Support Flower Speech, https://www.facebook.com/supportflowerspeech.

5 "Nay Phone Latt, Myanmar," PEN America, http://www.pen.org/defending-writers/nay-phone-latt.

6 Dangerous Speech Project, http://www.voicesthatpoison.org.

7 San Yamin Aung, "Hate Speech Pours Poison Into the Heart," The Irrawaddy, April 9, 2014, http://www.irrawaddy.org/interview/hate-speech-pours-poison-heart.html.

8 Facebook employees, in discussion with the author.

9 San Yamin Aung, "Hate Speech Pours Poison Into the Heart," The Irrawaddy, April 9, 2014, http://www.irrawaddy.org/interview/hate-speech-pours-poison-heart.html.

10 Jezebel Staff, "We Have a Rape Gif Problem and Gawker Media Won't Do Anything About It," Jezebel, August 11, 2014, http://jezebel.com/we-have-a-rape-gif-problem-and-gawker-media-wont-do-any-1619384265.

11 Jeremy Waldron, University Professor at NYU, makes a similar argument in his book The Harm in Hate Speech (Cambridge: Harvard University Press, 2012), for example.

12 Joel Johnson, comment on "We Have a Rape Gif Problem and Gawker Media Won't Do Anything About It," August 11, 2014, http://jezebel.com/im-in-the-middle-of-this-company-tech-thing-but-i-want-1619505494. See also Lauren Keating, "Jezebel slams Gawker for not addressing rape image complaint," Tech Times, August 12, 2014, http://www.techtimes.com/articles/12847/20140812/jezebel-slams-gawker-for-not-addressing-rape-image-complaint.htm.

13 "Controversial, Harmful and Hateful Speech on Facebook," May 28, 2013, https://www.facebook.com/notes/facebook-safety/controversial-harmful-and-hateful-speech-on-facebook/574430655911054.

14 "The Umati Project: Monitoring Dangerous Speech Online," http://www.ihub.co.ke/umati.

15 Prachi Gupta, "The worst reactions to Nina Davuluri being crowned Miss America," Salon, September 16, 2013, http://www.salon.com/2013/09/16/racists_call_miss_america_2014_a_terrorist/.

16 "University Of Illinois Students Respond To No Snow Day With Racism, Sexism On Twitter," Chicagoist, January 27, 2014, http://chicagoist.com/2014/01/27/university_of_illinois_students_res.php.

17 Michael Simeone, "Twitter Outrage, Charted: The Partial Anatomy of the #FuckPhyllis Trend, or Why I Don't Trust BuzzFeed," Suffen.us, January 29, 2014, http://suffenus.wordpress.com/2014/01/29/twitter-outrage-charted-the-partial-anatomy-of-the-fuckphyllis-trend-and-why-i-dont-trust-buzzfeed/.

18 "Asians in the Library - UCLA Girl (Alexandra Wallace) going wild on Asians ORIGINAL version," YouTube video, 2:51, Posted by "Sam Hong," March 13, 2011, http://www.youtube.com/watch?v=x0JKb_Cn1qc.

19 "A Racial Rant Inspires an Internet Balladeer," NPR, March 24, 2011, http://www.npr.org/2011/03/24/134827085/a-racial-quarrel-inspires-an-internet-balladeer.

20 "Ching Chong! Asians in the Library Song (Response to UCLA's Alexandra Wallace)," YouTube video, 4:15, Posted by "Jimmy Wong," March 15, 2011, http://www.youtube.com/watch?v=zulEMWj3sVA.

21 "Football fans go bananas in anti-racism protest," Al Jazeera: The Stream, April 28, 2014, http://stream.aljazeera.com/story/201404281742-0023677.

Facing Unthinkable Threats to Online Speech: Extreme Violence in Mexico and the Middle East

Ellery Biddle

When the slaying of James Foley dominated headlines last August, I could not help but think of Marisol Macías Castañeda,[1] the Mexican journalist whose severed head was found perched atop a computer keyboard in a city plaza, along with a note that read: "I am the Girl from Laredo and I am here because of my reports and yours."[2]

Macías had worked as the editor of a local newspaper, but prior her death in 2011 had also served as a leading contributor (under the pseudonym "La Nena de Laredo") at Nuevo Laredo en Vivo, a volunteer-driven site where citizens can file reports of drug-related violence that they'd witnessed in the northern border region. Signed "Z Z Z," the note beside Macías' decapitated body attributed the act to the criminal syndicate Los Zetas.

Macías' death was one in a series of brutal killings of northern Mexico residents who are using citizen and social media to report on drug violence. The tactics and visual presentation of brutality towards independent media workers by groups like the violent extremist organization known as ISIS are chillingly reminiscent of cases like Macías'.

Over the last four years, Syria and Mexico have been two of the most dangerous countries in the world for people doing journalism, regardless of whether they belong to established news outlets or report violence via social media. For years, large swaths of both countries have lain in unofficial jurisdictions controlled by highly organized groups of people, waging extreme violence in the interest of attaining power and profit.

The origins of these criminal organizations are distinct, as are the governments in these countries—human rights violations committed by the Syrian regime outstrip those of the Mexican government by several orders of magnitude, while the Mexican government has showed greater complacency in the face of cartels and organized crime than the Assad regime has toward ISIS. And although Mexico has paid lip service to the issue of extralegal threats to media workers, neither government has demonstrated a vested interest in protecting the rights and lives of these journalists. Both governments play a powerful role in enabling the conditions of possibility for these criminal organizations to thrive.

Caught between the brutality of these groups and repressive government tactics used to silence anyone seeking to uncover corruption or human rights abuses, many local journalists and news organizations have stopped reporting on these issues. In some cases, citizen media groups have stepped in to fill the void—projects like Syria's Radio ANA and sites like Nuevo Laredo en Vivo in Mexico have taken on the challenge of telling these stories to the world. In some cases, this has proven fatal. For journalists like Radio ANA's Rami al-Razzouk, who was kidnapped by ISIS fighters in autumn of 2013 and has not been heard from since, we simply do not know.[3]

From the perspective of the media and Internet rights community, it is hard to see much good com-

ing from directly asking groups like ISIS to stop persecuting media workers, much less anyone else. Though relatively scarce, campaigns addressing these issues tend to target government or intergovernmental organizations like the UN, or to raise public awareness about the problem, both worthwhile efforts, even if they reap limited results.

Among advocates for online rights, another common response to these events is something akin to paralysis. Stunned by the unthinkable nature of these acts, we find ourselves in a place where the tools and tactics that we typically deploy in the face of challenge seem useless. Our first thought is not, "this is a violation of the UDHR." The response is emotional, not rational—we are human.

Above all, we are disposed to think of these groups as being "crazy" or "psychopathic killers," as they're often described. But in order to develop a logical strategy for change in the face of this threat, we may need to rid ourselves of this powerful idea. Their goals and tactics may seem inhumane and unthinkable to most people, but they are still acting rationally. Nobel laureate and economist Gary Becker once argued that people engage in criminal behavior "not because their basic motivation differs from that of other persons, but because their benefits and costs differ." He argues that this determines their actions much more so than things like "biological inheritance," "family upbringing" or "disenchantment with society."[4] This model may be useful in looking at the problem at hand. When we develop an advocacy strategy, we map influential actors—government agencies, international organizations, tech and telecommunications companies, and human rights advocates typically fill in the grid. We identify their priorities, their strengths, their weaknesses. It is difficult to plug organized crime groups into this model—they're outside the law, they're not especially transparent, and it can be very difficult to figure out where they begin and where they end. But like most actors in our little grid, they seek to shore up power, money, and the kind of ideological influence that will help them to retain and expand their fields of power.

If we are going to campaign against this problem, or even write about it, we need to think in these terms. What government and intergovernmental policies and practices support the conditions that allow these groups to thrive? What are the economic drivers behind their dominance? Where do they get their weapons? Who supplies their fuel, food, water, housing? Who buys the drugs, weapons, and other goods that make up their business model? What surveillance technologies are they using to track the activities of media workers and human rights activists?

We must avoid becoming overly consumed by the activities of these groups where we see often see them first—online. And governments should, too—network shutdowns, online censorship, and mass surveillance have become routine responses to their acts that heavily infringe on the rights of all citizens to express themselves and report the news.

It may be time for open Internet advocates and citizen media groups start working in this frame of mind, a shift that could require us to zoom out from the increasingly narrow-seeming lens of fighting for digital rights. In the end, if we do not enjoy these rights "on the ground," we do not truly enjoy them at all.

Notes

1 Source (EXTREMELY GRAPHIC): Borderland Beat, "Woman Decapitated in Mexico for Web Posting," September 24, 2011, http://www.borderlandbeat.com/2011/09/woman-decapitated-in-mexico-for-web.html.

2 Original: "Yo soy la Nena de Laredo y aqui estoy por mis reportes y los suyos." Translation by author.

3 "Number of journalist kidnappings in Syria unprecedented," Committee to Protect Journalists, November 26, 2013, https://cpj.org/2013/11/number-of-journalist-kidnapping-in-syria-unprecede.php.

4 Gary S. Becker, "Crime and Punishment: An Economic Approach," from Essays in the Economics of Crime and Punishment, National Bureau of Economic Research, 1974, http://www.nber.org/chapters/c3625.pdf.

The Use of the Internet to Enforce Religious Hegemony in Saudi Arabia

Helmi Noman

Computerized faith-based activism—carried out by both individuals and by members of official religious groups—is increasingly becoming visible in the Middle East and North Africa. These actors harness the power of the Internet to enforce both their religious control and their ideological commitments. Their activities take a range of different forms, including organizing online campaigns to mobilize society against issues that do not conform to their religious beliefs, compromising the online presences of liberal intellectuals and political reformers, and crowdsourcing URLs of objectionable websites for blocking. This sort of activism often takes place under the banner of an Islamic religious doctrine known as hisbah, defined as the duty of enjoining good when it is neglected and forbidding evil when it is prevalent in society.

Segments of Saudi religious conservative community have the most notable faith-based activism online. They use the digital sphere to impose their religious values and perspectives on individuals and society, and to ensure there is no separation between the state and Islam as they interpret it. These conservatives are a cluster within the Saudi religious sphere, and are not representatives of the entire community. Some operate through a government-authorized religious police known as the Committee for the Promotion of Virtue and the Prevention of Vice; others work individually and independently of the committee. They use the fact that Islam is the state-sanctioned religion as their framework and the concept of hisbah as their mechanism to enforce religious hegemony. Examples of their activities highlight the scope and manifestation of the practice of hisbah online, and how pervasive and disruptive the activities can be.

An online group called The Channel of the Saudi Society describes itself on Twitter (@ksa12300) as "supporters of religion and the [practice of] hisbah; a shield to the homeland; a nightmare that irritates the liberals and seculars; and promotes virtue and prevents vice." The group says 30 muhtasibs (muhtasib is Arabic term for a person who practices hisbah) run the Twitter account, which also works as a crowdsourced operation that flags objectionable websites to government censors and what they see as violations of Islamic sharia to the concerned authorities. Objectionable local events that the Channel has brought to the attention of the authorities include public music performances, women driving cars, gatherings where men and women are mixed, and displaying of a Christmas tree in a shopping mall. The religious police often raid the reported events. A YouTube account run by the Channel posts videos showing raids by the religious police and other activities of the larger religious community. Examples of these clips include an amateur video showing a muhtasib raiding a public music performance and destroying a musical instrument belonging to a band member.[1] Another clip stigmatizes and shows photos of Saudi public intellectuals labeled by the Channel as misguided secular and liberal actors trying to corrupt the Saudi society.[2] The channel has also claimed to have used volunteer hisbah-driven hackers to break into religiously objectionable websites to acquire information about the websites' operators, leading to their arrest.

Other hackers have compromised Twitter and email accounts of Saudi activists over their liberal and perceived anti-Islam views. For example, the Twitter and email accounts of Saudi human rights ac-

tivist Souad al-Shammary were breached in April 2012 over her liberal views and for advocating for women's rights. To stigmatize her, the hackers leaked a photo retrieved from her email showing her posing with her hair uncovered in a public place, a behavior considered un-Islamic in the Kingdom. In the same month, the Twitter account of Saudi liberal writer Wael Alqasm was compromised to protest what the hackers called his Christian-influenced views and his stance that Saudi Arabia should permit building churches in the Kingdom.

The online activities of these conservatives do not only reflect a rift between segments of the religious community and elements of society, but also a fracture between these actors and certain government policies and what they consider government un-Islamic decision-making. In September 2014, they organized an online campaign that was harshly critical of the government for recognizing and celebrating a Saudi national day (September 23), arguing Muslims are not allowed to create and celebrate non-Islamic occasions that were not recognized by Prophet Mohammed. The campaign produced a video clip of several sheikhs saying it was forbidden for the government and the public to recognize a national day and to participate in related celebrations. In the same month, they organized another campaign on social media mobilizing public opinion against news that the government planned to lift the ban on movie theaters and to kickstart the cinema industry in the Kingdom.

The online activities of the conservatives do not go unchallenged, and counter-campaigns often emerge on social media. A campaign using an Arabic hashtag meaning "Stop the Saudi Society Channel" objects to the activities of the Channel and accuses the people behind it of violating the personal privacy of citizens and of intimidating activists. Opponents also use social media to highlight the excessive power of religious policing in public life. For example, Saudi female journalist and novelist Samar Al-Mogren tweeted in a photo of a fresh juice bar and café in the Kingdom displaying a sign that reads in Arabic: "Women are strictly forbidden from sitting on the chairs as per the instructions of the Committee [for the Promotion of Virtue and the Prevention of Vice]".[3] Al-Mogren commented on the photo saying, "They might as well abolish women from Saudi Arabia."

Photo tweeted by Samar Al-Mogren

The migration of hisbah, a concept more than 1400 years old, to the digital world in the 21st century is an interesting phenomenon. It highlights a duality of the Internet: while some actors use it to maximize its liberalizing effect on society, others use it to pervasively dominate public life, bolster conservatism of the society and maintain religious hegemonic control. Segments of the religious community use civic openings created by the Internet to wield their dominance and influence on society and to silence and combat others from exercising their civic rights both online and offline by assigning and enforcing their conceived religious appropriateness to personal and collective political, social, and cultural activities.

Notes

1 "الشيخ ابو مالك يوقف حفل غنائي بالجوف [Sheikh Abu Malik stops a musical performance in Al-Jawf region]," YouTube video, 1:53, Posted by "قناة المجتمع السعودي [The Channel of the Saudi Society]," May 2, 2010, http://www.youtube.com/watch?v=B2mM0v56_mA.

2 "هيئة الأمر بالمعروف والنهي عن المنكر" 74 عاماً من الجهاد الميداني المبارك [Committee for the Promotion of Virtue and the Prevention of Vice: 74 years of Blessed Field Jihad]," YouTube video, 8:47, Posted by "قناة المجتمع السعودي [The Channel of the Saudi Society]," June 22, 2014, http://www.youtube.com/watch?v=k96ae_BJbcg.

3 Samar Al-Mogren, Twitter post, March 1, 2014, 6:55 a.m., https://twitter.com/s_almogren/status/439730615613915136/photo/1.

#BBUM and New Media Blacktivism

Clarence Wardell

On November 7, 2006, the people of the state of Michigan voted 58% to 42% to prohibit the consideration of race, among other criteria, in the admissions process at state universities. The vote marked the culmination of efforts begun by Ward Connerly and the Michigan Civil Rights Initiative following the 2003 Supreme Court rulings in twin cases (Gratz v. Bollinger and Grutter v. Bollinger) that targeted the University of Michigan's admissions process. Connerly's stop in Michigan was preceded by a similar effort in California, where he helped pass Proposition 209 in 1996.

Following the 2006 vote, the percentage of black students enrolled in Michigan's freshman class dropped from 6.4 percent that year to 4.6 percent in 2013. This mirrored the pattern seen in California at the state's flagship universities—UC Berkley and UCLA—after the passage of Proposition 209. Connerly's work effectively set back the gains of the University of Michigan's Black Action Movements (BAM I, II, and III). Most famously, BAM I saw black students shut down the university for 18 days in 1970 to call attention to what they perceived as slow progress towards integration.

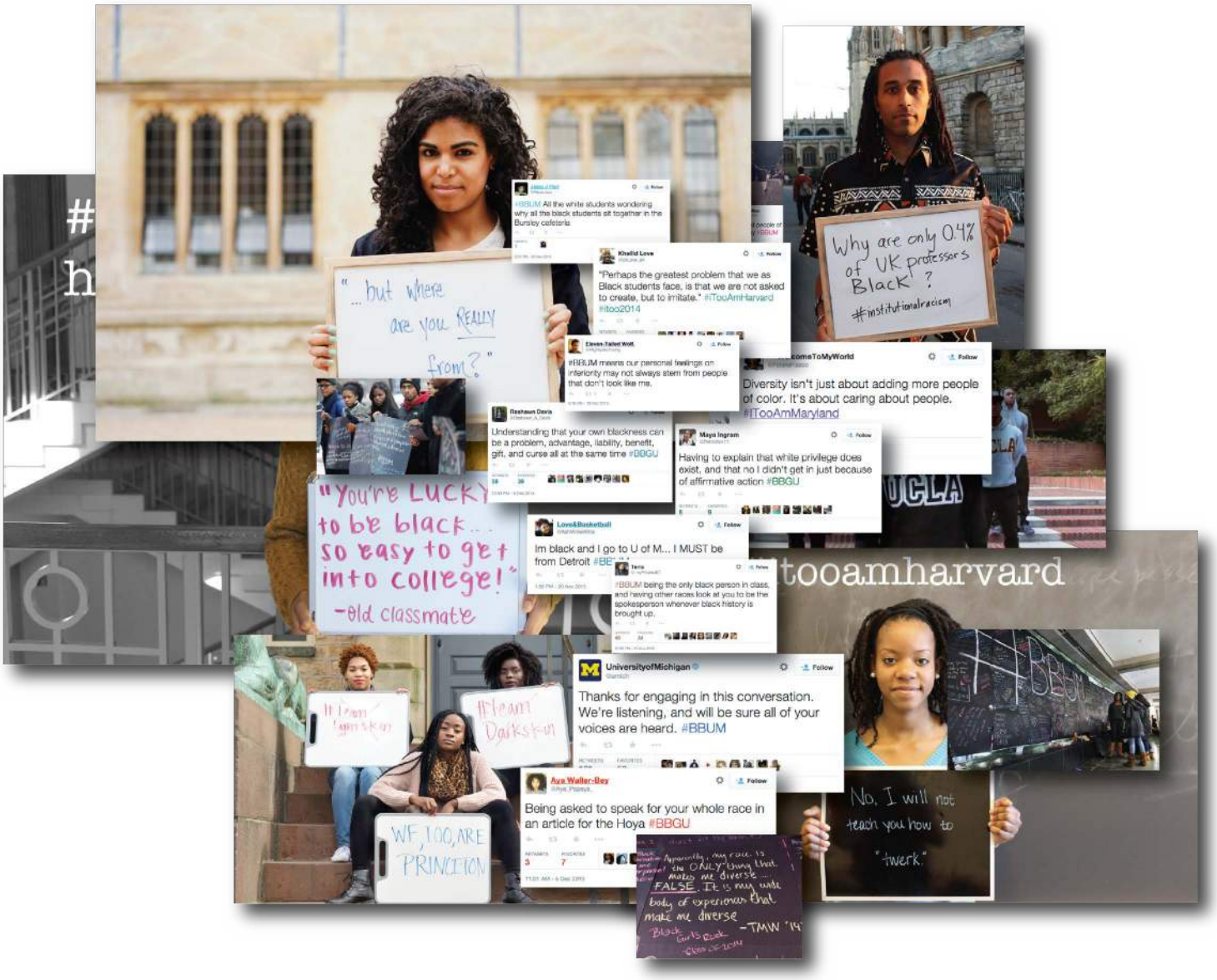
In November 2013, Michigan's Black Student Union, upset over their dwindling numbers on campus and what they found to be an increasingly hostile environment, convened student leaders to discuss how they could make their voice heard. They considered a retread of the tactics that worked for BAM over forty years earlier, but in part fearing low initial participation, they opted to focus on a low-barrier to participate Twitter campaign using the hashtag #BBUM (Being Black at the University of Michigan). The idea centered on black students simply sharing their experiences at the university, good or bad, on Twitter using the tag. In some ways, it echoed a similar UCLA effort, a few weeks prior, that saw 12 students release a spoken word video on YouTube. The video, entitled "The Black Bruins," eventually garnered over 2,000,000 views. The Michigan campaign launched on November 19, 2013, and within one hour was trending nationally across Twitter. Local and national media outlets soon picked up the story, and by 10pm that day, there were over 10,000 Tweets containing the hashtag.

While #BBUM initially started with a small but densely connected group of students in Ann Arbor, MI, the campaign was ultimately amplified and sustained by a broader public consisting of black students and alumni of universities across the world, all connected by similar experiences at their respective schools. In many ways, the #BBUM campaign constituted a major inflection point in the long history of black student activism on college campuses across the country, validating a new type of engagement. It was preceded by UCLA's campaign a few weeks earlier, and followed by similar campaigns at other schools such as Georgetown University, and eventually Harvard and Oxford's "I, Too, Am" photo campaigns in early 2014. All of these campaigns successfully leveraged social media platforms to share images and raise awareness about similar issues far beyond the campuses on which they began. To this point, Harvard students held a "blacktivism" conference in October 2014 to build on the momentum of these new media campaigns.

Ultimately, the #BBUM campaign—which students followed with on-the-ground organizing work as

well as a YouTube video listing student demands of the university—gained such traction that the New York Times ran a front page story. Moreover, the effort compelled administrators at the university to respond to student concerns, leading them to hold standing meetings with the student organizers for the remainder of the 2014 school year.

Beyond its effect in Ann Arbor, the #BBUM campaign demonstrated the importance and power—particularly for minority communities—of connecting digital activism and the breadth of participation that it affords, with the tactics pioneered by a previous generation of students.



Images and tweets from the #BBUM, #BBGU, and "I, Too, Am" campaigns

How Activism and the Internet Can Change Policy

James Losey

On September 10, 2014, 40,000 websites participated in an "Internet Slowdown" campaign to draw attention to the net neutrality debate in the United States. The debate, centering on how the Federal Communications Commission will apply regulatory authority to protect an open Internet, is the latest issue in which online collective action has targeted Internet policy concerns. For example, a previous online protest on January 18, 2012 voluntarily censored 115,000 websites to target the Stop Online Piracy Act (SOPA) and the PROTECT IP Act (PIPA), two copyright enforcement bills. In the following months, online organizing led to large-scale street protests against the Anti-Counterfeiting Trade Agreement (ACTA) in Europe.

Numerous scholars have discussed different virtues and drawbacks of digitally mediated engagement. Evgeny Morozov argues that online engagement amounts to "slacktivism" and detracts from meaningful offline action.[1] By contrast, Ethan Zuckerman argues that digital media supports "participatory civics" in which individuals can selectively engage with issues with varying degrees of independent thinking.[2] Political scientists Lance Bennett and Alexandra Segerberg argue that digital media supports a "logic of connective action": personalized action with loose or little central organization supported through digital media and social networks.[3]

However, focusing only on easily visible online advocacy misses the critical contributions of institutional advocacy in achieving democratic change. The SOPA/PIPA blackout and ACTA protests were both successful policy interventions—SOPA and PIPA were both withdrawn from Congress and ACTA was rejected by the European Parliament in part due to public advocacy efforts like mobilization of publics and online engagement. At the same time, complimentary actions such as gaining access to government bodies, lobbying, and targeting decision makers are what Sabine Lang defines as institutional advocacy.[4] Institutional advocacy, concomitant with public advocacy, is a critical component of democratic change.

Take the opposition to SOPA and PIPA as an example. The bills were once seen as enviable but quickly withdrawn mounting opposition that peaked with the online protests. The timeline indicates the importance of online protests. During the months preceding the online protests, groups including the Electronic Frontier Foundation (EFF), Public Knowledge, Demand Progress, and Fight For the Future helped amplify concerns over the legislation in the networked public sphere.[5] Specific events such as a boycott of domain register Go Daddy and the January 18 blackout raised the public profile of the debate.[6] In addition to these public advocacy efforts, less visible organizing in Washington, DC seeded opposition in Congress. For example, EFF organized a letter to members of Congress citing the security concerns of SOPA, which inspired the meme "bring in the nerds," highlighting the ignorance of the technical ramifications of SOPA during a December 15, 2011 Judiciary Committee hearing.[7] Google doubled its lobbying expenditures, and Wikipedia registered to lobby for the first time.[8] New participants to intellectual property debates such as human rights organizations organized a letter to members of Congress and held events on the Hill stressing the ramifications the bills posed to Internet freedom.[9] The blackout also endeavored to more than raising public awareness; it also en-

couraged US Internet users to engage their representatives. On the day of the blackout, I was on the Hill with a cadre of human rights organizations meeting with Senate staff to discuss the international implications of SOPA and PIPA. As we waited in each office, the phones were ringing off the hook, and staff informed us they were overloaded with opposition to the bills.

The rejection of ACTA by European Parliament also demonstrates a combination of public and institutional advocacy. Two major days of protest against ACTA that took place across nearly 200 European cities were coordinated through loose, ad-hoc networks . Combined with particularly newsworthy events such as members protesting in Poland's Parliament, the visibility of ACTA and broader public understanding of the potential harmful impact to the Internet from early drafts of the Agreement grew. However, in addition to public advocacy campaigns, civil society organizations strategically bridged these efforts to the debate inside European Parliament. Groups like La Quadrature du Net and European Digital Rights met with Members of European Parliament (MEPs) and organized trips for volunteers to be present during hearings and committee votes.[10] MEPs, who months prior were not even aware of ACTA, voted to reject the trade agreement.

As of this writing, the net neutrality debate continues in Washington, DC, but looking beneath the surface of the September 10 Internet Slowdown demonstrates the institutional advocacy efforts underway. For example, during the slowdown, participants were invited to contact their members in Congress, the White House, and the FCC with their support for net neutrality. At peak during the slowdown, Congress received an average of 1,000 calls per minute from Internet users engaged through the online protest.[11] Additionally, the FCC has received over 3 million comments, a record number.[12] One bump came following a mention of the issue by John Oliver on his show, and an order of magnitude more comments were filed just before the deadline.[13] An analysis by the Sunlight Foundation found that less than 1% of the comments completely oppose net neutrality.[14]

Without question, the Internet is a powerful tool for organizing and communication. But as these examples demonstrate, democratic change for Internet policy results from a combination of both public and institutional advocacy. For researchers, these events serve as a reminder that understanding Internet activism requires investigating both visible protests as well as less visible actions targeting decision-making processes. Similarly, civil society seeking change must leverage public engagement to encourage individuals to address decision makers. As long as governmental institutions are architected based on old hierarchies with traditional feedback mechanisms, phone calls and face-to-face meetings will continue to be critical tactics for democratic change.

Notes

1 Evgeny Morozov, The Net Delusion: The Dark Side of Internet Freedom (New York: PublicAffairs, 2012).
2 Ethan Zuckerman, "New Media, New Civics?," Policy & Internet 6.2 (2014): 151-168.
3 W. Lance Bennett and Alexandra Segerberg, The logic of connective action: Digital media and the personalization of contentious politics (Cambridge: Cambridge University Press, 2013).
4 Sabine Lang, Civil Society, and the Public Sphere (New York: Cambridge University Press, 2013), 23.
5 Yochai Benkler, et al., "Social mobilization and the networked public sphere: Mapping the SOPA-PIPA debate," Berkman Center Research Publication 2013-16 (2013).
6 Tom Cheredar, "Go Daddy loses over 37,000 domains due to SOPA stance," Venture Beat, December 24, 2011, http://venturebeat.com/2011/12/24/godaddy-domain-loss/.
7 Andrew McDiarmid and David Sohn, "Bring in the Nerds: The Importance of Technical Experts in Defeating SOPA and

PIPA," in Hacking Policits: How Geeks, Progressives, The Tea Party, Gamers, Anarchists and Suits Teamed UP to Defeat SOPA and Save the Internet, eds. David Moon, Patrick Ruffini, and David Segal (New York: OR Books. 2013).

8 Viveca Novak, "SOPA and PIPA Spur Lobbying Spike," Open Secrets, January 26, 2012. http://www.opensecrets.org/news/2012/01/sopa-and-pipa-create-lobbying-spike/.

9 "Letter from International Human Rights Organizations re: SOPA and PIPA," November 15, 2011, https://s3.amazonaws.com/access.3cdn.net/ea0af5a75bcbfe15c4_v0m6bxvv4.pdf.

10 James Losey, "The Anti-Counterfeiting Trade Agreement and European Civil Society: A Case Study on Networked Advocacy," Journal of Information Policy 4 (2014).

11 Battle for the Net, https://www.battleforthaenet.com/sept10th/.

12 Brian Fung, "The FCC has now received 3 million net neutrality comments," The Washington Post, September 15, 2014, http://www.washingtonpost.com/blogs/the-switch/wp/2014/09/15/the-fcc-has-now-received-3-million-net-neutrality-comments/.

13 Gigi B. Sohn, "FCC Makes Open Internet Comments More Accessible to Public," Official FCC Blog, August 5, 2014, http://www.fcc.gov/blog/fcc-makes-open-internet-comments-more-accessible-public/; minimaxir, "Number of Comments the FCC Has Received Daily Regarding Net Neutrality [OC]," Reddit, r/dataisbeautiful, August 6, 2014, http://www.reddit.com/r/dataisbeautiful/comments/2cskdc/number_of_comments_the_fcc_has_received_daily/.

14 Bob Lannon and Andrew Pendleton, "What can we learn from 800,000 public comments on the FCC's net neutrality plan?," Sunlight Foundation, September 2, 2014, http://sunlightfoundation.com/blog/2014/09/02/what-can-we-learn-from-800000-public-comments-on-the-fccs-net-neutrality-plan/.

Narratives of Conflict: What the 2014 Gaza War Can Tell Us About Discourse on the Internet

Sands Fish and Dalia Othman

This summer, the war in Gaza and Israel dominated coverage on many news sites. The war lasted for 50 days and resulted in over 2,000 deaths (mostly civilians), thousands of injuries, and overwhelming destruction. Media reports varied in their coverage, with the stories spanning from Hamas' rockets being fired into Israel to the toll this war has had on Palestinian children, the destruction of UNRWA schools, and more. Using digital media analysis platform Media Cloud, we tracked media coverage of the war to gain a better understanding of the different topics that emerged and the frames that were adopted by different media outlets.

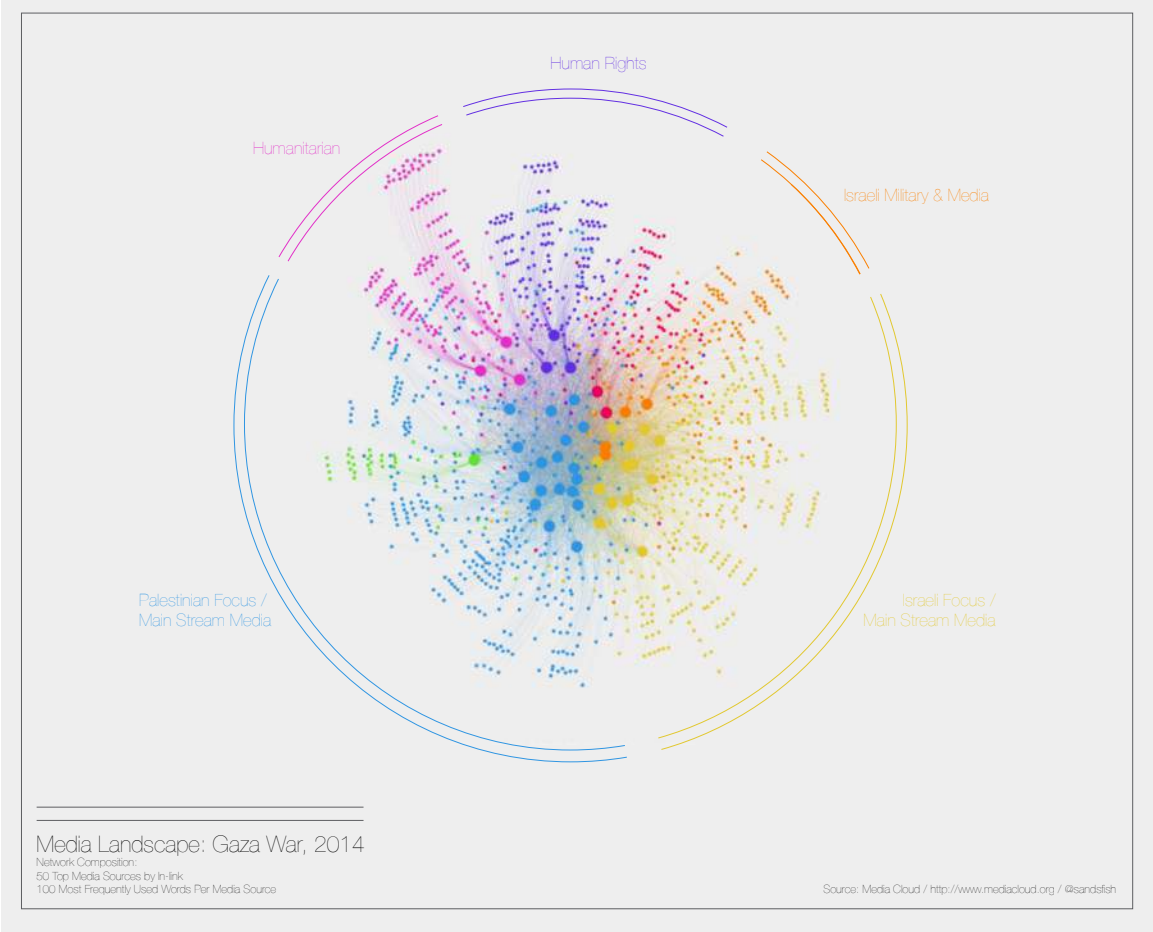
Through this analysis we are able to draw a map of the media landscape, highlighting the relationships between different media sources based on the similarities and differences in the language that they adopt. We are able to identify five meaningfully distinct clusters: one cluster includes large media sources from the US and UK that align with Israeli narratives, while another cluster of western media hews more closely with Palestinian perspectives. Three other clusters are comprised of the Israeli military, human rights organizations, and relief organizations.

For our analysis, we drew on a corpus of 80,000 stories that were collected for this study. From this corpus, we focused our attention on the stories published by the 50 most prominent English language sites, as measured by the number of links from other media sources. We employed a network structure that clusters media sources by the content of their stories and creates a visual representation of the media landscape in which influential media sources are connected to one another based on the words that they use most frequently within the bounds of a given topic. Using network theory, we constructed and analyzed the ways in which media sources are affiliated via shared vocabulary. We drew a network map based on the 100 most frequently used words from each media source. A link was created from a media source node to a target node representing the word the media source used frequently, appropriately weighting the link based on the frequency of usage. We then used a community detection algorithm, allowing us to see patterns of term usage in the text of online discourse. Media sources, in this way, are connected via shared language and can be laid out based on their connective strength. The resulting map, in this case, generated five distinct community clusters.

Focused on Gaza, this network map revealed communities of media sources and vocabulary that, when analyzed, uncovered a number of frames deployed in the overall coverage of the war. We were able to discern that, while the average reader might assume there is simply one Israeli frame and one Palestinian frame, the media landscape is much more complex.

Upon further investigating the communities, one can see what makes each of them unique is based on the media source's frequent use of certain terms. The fact that Relief Web (a UN affiliated site) is one of the only media sources to use ambulances frequently in their coverage describes the predominant narrative this media source focuses on. Assertions can also be made about media source similarity within and across these communities by analyzing the co-occurrence of word usage in pairs or

clusters of media sources. An illustrative example of this is the use of distinct terms such as *breaches, crimes,* and *disproportionate* linked to Amnesty International and Human Rights Watch. These terms help define the "Human Rights" community.



Two of the clusters (Palestinian Focus and Israel Focus in the figure above) are primarily comprised of mainstream media sources. The split in these two clusters is evidently based on the affiliation with Israeli or Palestinian sources and exposes a slant in the coverage of the war associated with different media sources. The Palestinian Focus cluster contains both Maan News, a Palestinian mainstream media source, and Mondoweiss, a pro-Palestinian left-leaning American Jewish site, in addition to sites such as Al Jazeera and the UK's The Independent. The language used more frequently by these sites include words such as *evacuate*, *children*, and *casualties*, terms that focus on the toll of the war. The Israel Focus cluster includes Israeli media sites such as Jerusalem Post and the National News of Israel, along with CNN and the US right-wing site Breitbart. The media sources in this cluster more frequently use terms such as *tunnels*, *sirens*, and *arms*, terms indicating a greater focus on Hamas' actions against Israel. Both clusters are comprised primarily of US and UK mainstream media sites and use terms common across all coverage of the conflict; however, the divide between clusters indicates a slight slant towards either perspective.

Two topical clusters revolve around humanitarian and human rights issues, respectively. The Hu-

manitarian cluster includes three sources: the United Nations, UNRWA (UN Palestinian Refugee Agency), and Gisha, an Israeli legal center for freedom of movement. These sources used words such as *psychosocial*, *hygiene*, *sanitation*, *truckloads*, and *shortage*. This cluster is distinct from the Human Rights cluster that includes Amnesty International, Human Rights Watch, and B'Tselem, an Israeli human rights organization. This cluster more frequently uses a separate set of terms, including *breaches*, *detainees*, *shrapnel*, and *violations*, that are more commonly used in the human rights community.

In addition to the Israel Focus cluster, there is also a separate cluster comprised of Israeli military and Israeli mainstream media sources. This cluster is dominated by the IDF (Israeli military) blog and spokesperson site alongside news sites such as Ynet and Times of Israel. The terms used more commonly in this cluster, such as *soldiers*, *battlefield*, and *brigade*, carry military connotations.

Notably absent from the map is a cluster comprised primarily of Palestinian media sources. This stems in large part from the relatively small number of Palestinian sites that were represented in the top 50 media sites contributing to coverage of this issue; three pro-Palestinian sites compared to eight Israeli sites. The Palestinian media sites that are included in the network map are included because they drew attention from the Western mainstream media, as demonstrated by the number of inlinks to these sites.

Using texts from thousands of online stories, we were able to detect slants in mainstream media's coverage toward Israeli and Palestinian narratives. The Gaza war provided an ideal case study for better understanding how to analyze discourse online. These are initial findings resulting from the exploration of both story and tool. Moving forward, we plan to increase the robustness of the visualization and our confidence in its representation of substantive discursive trends. With the growth of analytical tools and methods such as this, the insight that can be gained from study of the large-scale text sourced from the networked public sphere will only expand. The opportunity for qualitative analysis of discourse online using automated quantitative tools provides a deeper view into human communication than has ever been available.

Who Do We Trust When Talking About Digital News in Spain?

Charo Sádaba

Trust is hard to obtain and maintain, but at the same time, it has extraordinary value for governments, institutions, and businesses. In the digital age, amidst an overdose of information and sources, trust is still important not only for news and media companies but also for readers eager to find a reliable method to stay informed and updated.

According to the Edelman Trust Barometer, Spaniards' level of trust in mass media dropped from 50% to 40% over the past year.[1] This drop is worse for media than for government institutions (-6%) or companies (-2%), although the initial levels of trust were lower in both of these cases.

According to the Digital News Report 2014, edited by the Reuters Institute of University of Oxford, only 23% of Spanish online news readers would subscribe to a digital news service because of the brand, the lowest level among all the countries involved in the study.[2] But this is not a lost battle for media companies, as brands still play a crucial role in the online news industry: 46% of online news readers in Spain go directly to branded news sites to read the news. For 55% of these readers, the brand is important for creating trust, according to the DNR 2014 report. However, media companies should take into account that Spaniards give more credit and a more relevant role to the individual journalists instead of the media brand (61% vs. 55%), a phenomenon that is only happening in Spain, according to the available data.

Why media brands are not enough to sustain online traffic and trust is an interesting debate, given that several reasons could be provided. Spain is in the middle of a harsh institutional crisis affecting political, economic, and social spheres. In the past few years, citizen and consumer dissatisfaction with political parties, trade unions, banks, and corporations has been growing at the same pace that trust in these institutions has been collapsing, according to the Edelman Trust Barometer. Media companies in Spain that traditionally have been very close to the structured powers are also suffering the readers' disaffection. Additionally, recent reforms to the Intellectual Property Law have given media producers their long-claimed right to receive monetary compensation from news aggregators or anyone using or quoting original content produced by them (widely known as the "Google News tax"). While these demands may be legitimate, the new law has been received poorly by users fearful about being asked to pay if they share or use content on their personal blogs, and Google News has announced that it will be pulling out of Spain rather than pay publishers.[3] How media brands could be affected by being in the middle of the battered relation between regulatory efforts and Internet users in Spain is yet to be known.

If brands want to maintain their leverage in the online sphere, more proactive actions should be taken to increase their value in the eyes of the readers. Losing this opportunity to reinforce trust could be both expensive and definitive for media brands.

Notes

1 2014 Edelmen Trust Barometer, http://www.edelman.com/insights/intellectual-property/2014-edelman-trust-barometer/.
2 "Digital News Report 2014," Reuters Institute for the Study of Journalism, http://www.digitalnewsreport.org/.
3 Justin Ellis, "Google News closes up shop in Spain," Nieman Lab, December 11, 2014, http://www.niemanlab.org/2014/12/google-news-closes-up-shop-in-spain/.

Why Blogs Still Matter to the Young

Alison J. Head

Technology writers have declared the death of blogs and the evidence, it seems, is undeniable. Readership has declined dramatically as content that once was the bedrock of the blogosphere has migrated to sites like Tumblr, Twitter, or Facebook.[1]

But this year, when we conducted in-depth phone interviews with 63 recent graduates from 10 US colleges and universities as part of a national study on lifelong learning, we discovered that the death notice for blogs might be premature.[2] Young graduates, in fact, said they placed a high value on blogs when we asked if, and how, they kept learning after college.

Utility is key to understanding how and why young graduates rely on blogs for supporting their lifelong learning as they make the transition from college into real life. Our interviewees admitted to looking for "specifics" and "how-to information" they could directly apply in the workplace, the community where they lived, or their personal lives. This was often to shore up knowledge and to close their skill gaps. Graduates also wanted practical and no-cost information that they could call up quickly and use.

We found, however, graduates were selective about the blogs that they choose to consult. Many said they followed blogs after having carefully vetted them using a range of different approaches. One interviewee said he started reading a digital marketing guru's blog after first learning about him in a New York Times business article. Another interviewee, who is setting up her own graphic design business, said she is following a well-known entrepreneur's blog.

Still another young graduate mentioned doing a Google search and culling through results to find a credible blog about setting up first-time personal budgets after college. The comments posted on blogs, she said, helped her figure out which solutions worked over time and, ultimately, whether or not they were feasible for her.

At a time when bloggers may be posting far less on their WordPress or Blogger sites than they once were, our research tells us young adults may still turn to blog content over mainstream media sources for a variety of reasons.

Blog content is a good value with up-to-date information from insiders, according to interviewees. Many said they could not pay to learn from tutors or professional experts available to others in "real life." Blogs were an affordable source of the know-how they needed. Others said there is an authenticity and candor to blog content because writers rarely are compensated, unlike the writers from the mainstream media publications that they tended to mistrust. Interestingly, none of the interviewees mentioned sponsored reviews, which are a form of advertising on some blogs.

Most graduates we interviewed prioritized their search for lifelong learning sources by looking for util-

ity as well as for multiple voices writing about the kinds of things twentysomethings need to know. There are, of course, a myriad of online sources with this kind of shared utility for lifelong learning, such as online forums, webinars, social media, video-sharing sites, and MOOCs.

Our findings, however, suggest that blogs, far from dead, are thriving, but in a different form, at a time when sites like Coursera, Google Helpouts, and Instagram brim with the promise of luring younger online users away from older traditional platforms. These newer online venues may simply not be enough to provide lifelong learners with the kind and quality of information recent graduates seek.

Based on our interviews, we suspect that the overall quality and depth of blogs that have not migrated to social media platforms may be filling a gap with more information rich content and less of the self-absorbed opinion and personal musings of the past.

Notes

1 See Verne Kopytoff, "Blogs Wane as Youth Drift to Sites Like Twitter," The New York Times, February 20, 2011, http://www.nytimes.com/2011/02/21/technology/internet/21blog.html; Jason Kottke, "The Blog is Dead, Long Live the Blog," Nieman Journalism Lab, December 19, 2013, http://www.niemanlab.org/2013/12/the-blog-is-dead/; and Felix Gilette, "Department of Blogging Extinction: Technorati Rankings Are Dead," Business Week, June 24, 2014, http://www.businessweek.com/articles/2014-06-24/department-of-blogging-extinction-technorati-rankings-are-dead.

2 Project Information Literacy (http://projectinfolit.org) conducted this research in collaboration with the University of Washington's Information School and in affiliation with the Berkman Center for Internet & Society at Harvard as part of a two-year study on lifelong learning, funded by the Institute of Museum and Library Services. Testing of these qualitative trends will occur with quantitative data collected from a large-scale survey PIL administers to recent graduates at 10 US colleges and universities. A findings report will be released in December 2015.

The Podemos Phenomenon

Jordi Rodriguez Virgili

Podemos (We Can Do It) is a Spanish political party founded in March 2014. Just two and a half months later, it obtained 1,245,948 votes (7.97%) and 5 seats in the Spanish elections for the European Parliament, held on May 25. Podemos became the fourth most popular party in the country. This success does not seem temporary: The latest polls place it as Spain's second largest political force, well positioned to challenge the leftist leadership of the historic Spanish Socialist Labor Party (PSOE).

Although it may seem that the rise of Podemos was sudden and spontaneous, the party was not built from scratch. It relied on the network of activists established during the 15M mass demonstrations in 2011-2012. The 15M was a social movement expressing growing political disaffection among Spanish citizens. Podemos was able to gain support by gathering a number of scattered but very active groups—such as 15M, EnRed, DRY, the PAH, Marea Verde, and Rodea el Congreso—under one banner. Podemos channelled the craving for reform and attracted different population sectors particularly hit by the economic crisis that share a general dissatisfaction with Spain's current economic and political situation. Half of Podemos voters are under 40 years old, more than two-third position themselves on the left, and more than half are male. In sum, they are well informed, politicized, and "socially connected" voters.

This burgeoning political party is spearheaded by Pablo Iglesias, a political science professor who regularly participates in political talk shows on Spanish TV. In Spain, almost three out of four citizens regularly receive their news via television. This is how Iglesias acquired visibility and reached a wider audience.

Iglesias has declared on Twitter that "To claim that the success of Podemos is based on the frequency of my TV appearances undermines what we stand for."[1] The impact of the Podemos communications strategy was enhanced by viewers using multiple screens: transitioning nonstop between the TV screen and the screens of smartphones, tablets, and laptop computers. The average Podemos voter is characterised by their frequent use of social media. While 95% of Podemos voters use the Internet to become informed about topics, more than half of Popular Party (PP) and PSOE voters don't even have an e-mail address.

Podemos was established out of a challenge to empower citizens—an ever-present underlying goal reflected by its use of crowdfunding as a key fundraising strategy. The party's three-fold campaign platform was a collective effort that included online discussions and invitations to make individual contributions, amendments proposed collectively by different "Circles," and an online referendum on the proposed amendments. These circles, acting as grassroots organizations, together with a digital approach to disseminating information, resemble the framework used by Beppe Grillo, founder of the Five Star Movement in Italy, which was based on citizen and street-level activism.

The increasing demand for new politics goes hand in hand with that for new forms of communication.

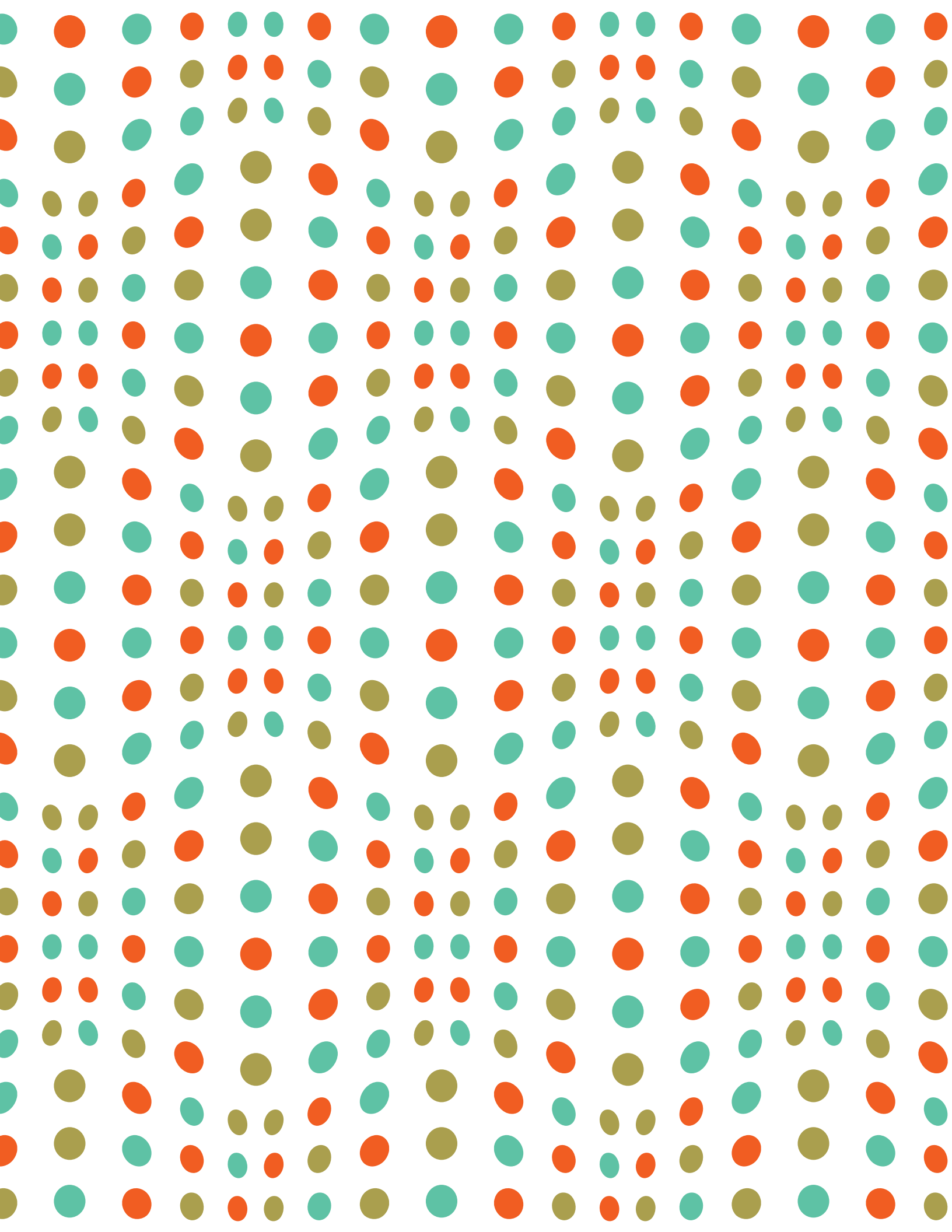
The rhetorical approach of Pablo Iglesias, which includes both a distinctly populist tone and an optimism that Podemos can bring about true change, is well suited to the brevity and emotiveness of the digital language.

This is a true, real-life retelling of the David and Goliath story, where an outsider confronts establishment power, or the so-called upper caste. Along those lines, Podemos has positioned its stance around the economic crisis, issuing messages reflecting its position: "victims vs. perpetrators, old vs. new, the upper caste vs. the people."

The current challenge for Podemos lies in reconciling open participation with the creation of stable management structures. Podemos has taken a rapid and unconventional path toward becoming a political force in Spain and must now turn its attention to creating a political party out of a campaign team.

Notes

1 Pablo Iglesias, Twitter post, May 28, 2014, 12:19 PM, https://twitter.com/pablo_iglesias_/status/471732614399664128.



INTERNATIONAL ISSUES: TRANSNATIONAL LEGAL TENSIONS AND INTERNET GOVERNANCE

Robert Faris and Rebekah Heacock Jones

The flow of data across international borders has been an undisputable engine of innovation in the digital economy and facilitated a myriad of tools, applications, and platforms used by citizens, businesses, and governments. Information freely flowing out of the reach of governments and without regard for international borders has long inspired cyber-utopians and cyber-libertarians. The questions of jurisdiction and control—whether governments should or could control the flow of information—have fueled debates over Internet governance and the role of government in digital affairs. While governments have done much over the past two decades to reassert their sovereignty in cyberspace, the complexities of regulating technologies that have little regard for geography continue to shape debates over Internet policy and governance. The relationship between national governments and Internet intermediaries constrains what a majority of Internet users are able to do on the Internet; only a relatively small cadre of users has the motivation and technological ability to overcome the technological limitations put into place by governments.

Where citizens use Internet services hosted domestically—social media, social networking, file sharing, blog hosts, email services, and others—the regulatory and jurisdictional questions are greatly simplified: governments are a phone call or subpoena away from gaining access to information needed to enforce local laws. The limited ability of governments to hold sway over foreign companies is a principal reason that the Internet is the way that is today. In China, authorities blocked access to western Internet services, including Twitter, Facebook, and YouTube, which helped to ensure that domestic alternatives control the market, giving the authorities the ability to enlist the help of intermediaries in policing content in a manner that outside companies would resist. The failure of YouTube and Twitter to respond to content filtering requests in Turkey led to the frequent blocking of those sites there. In Thailand, an agreement was reached with YouTube to block certain videos for Thai users that ran afoul of lese majeste laws, while these videos remained available elsewhere. Agreements reached with Google and Yahoo! enabled the removal of search results that pointed to content illegal in Germany and France, including hate speech and content related to Nazis. These agreements have formed the basis for broader systems to block content regionally where valid requests are submitted by legal authorities. These restrictions are notoriously flimsy—choosing an alternative country setting will gain access to the locally banned information—but offer an imperfect solution to a hard problem.

Efforts by sovereign governments to limit access to certain types of information within their borders and to secure user information housed in overseas servers will continue to strain this uneasy and constantly shifting equilibrium. The balance is maintained by adjustments to a small number of policy options: 1) maintaining international information flows by harmonizing standards across countries; 2) accommodations by international intermediaries to respect national differences; and 3) balkanization where these other two options fail. For countries around the world, the Internet has always been and will continue to be opt-in politically and socially. In terms of physical infrastructure and architecture, it continues to be opt-out; by default everything passes through the network unless measures are taken to create limits. Fortunately, there is a strong incentive for most countries to continue exchang-

ing information across borders using standard Internet protocols, which has limited the moves toward balkanization.

International power dynamics are impacted by the decisions of consumers and the ability of companies to attract users to their services. By virtue of the early and continued success of its technology companies, the United States has long held a favorable position, allowing it to maintain a strong stance of openness while also avoiding most jurisdictional problems and having access to user information when desired. The United States' commitment to safeguard free speech has been exported as the default option for other nations. By virtue of this trajectory, many countries have arguably allowed more online speech, accepted anonymous and pseudonymous speech, and permitted viewpoints that fall far enough outside of their social norms that they would not be tolerated in offline venues. The comingling of free speech with digital commerce has been a significant impediment to more decisively and comprehensively enforced national standards on acceptable speech. There continues to be a fair amount of friction in cross-border data requests, for example in the formal mechanisms in place to handle data requests across borders,[1] which has provided additional protection for many Internet users from their own governments.

The constantly evolving unilateral and bilateral arrangements between countries and companies determine most of the rules and standards for what passes across borders on the Internet, where servers with user data reside, and where company personnel are situated. Another complex set of policies and decisions are made at the international level that fall under the rubric of Internet governance. The set of issues cobbled together under this umbrella term generally includes the allocation of domain names, technical standards, and other areas related to technical coordination, and typically encompasses the activities of many organizations, including ICANN, IETF, IAB, W3C, and ISOC, among others. There is disagreement about the proper scope of Internet governance; some advocate for a narrow conception while others argue that it should include consideration of human rights as well as social and economic issues.

These Internet governance institutions are buoyed by the principles and practice of a bottom-up multistakeholder governance model. At its finest, multistakeholder governance is a sophisticated 21st century model that combines a thorough understanding and balancing of different interests and perspectives into an integrated decision-making process that enables consensus building around complex technological issues and brings to bear decentralized expertise. At its worst, multistakeholder governance is a fig leaf that conceals the back room deals that serve powerful interests and pay little heed to the interests of the broader global Internet community. This set of institutions and policies have held together and functioned reasonably well through the years despite unending criticism over the dubious legitimacy of the organizational structures by the standards of international law and weak mechanisms for ensuring accountability to the global Internet community. The system has sought legitimacy instead through process, primarily open participation and transparency, and outcome. While the imperfections of these governance institutions have been laid bare, it is not clear whether there are better alternatives in the offing.

The past year represents in some ways an existential crisis for Internet governance and its roots in multistakeholder governance. The pending expiration of a key contract with the United States govern-

ment has set in motion a search for modifying the current structure to better reflect the international responsibilities of ICANN.[2] (This contract is a core argument against the legitimacy of ICANN to make decisions of international import, and also a critical thread of comfort for those who worry that authoritarian governments will co-opt Internet governance in order to water down existing standards of openness and provide political support for greater content restrictions).

The Snowden revelations and the ICANN transition have sparked a surge in Internet governance-related activity. In October 2013, the leaders of the aforementioned Internet governance institutions released a statement on the future of Internet cooperation, warning against balkanization and calling for a sustained multistakeholder effort to address Internet governance issues.[3] Days later, after consulting with the President and CEO of ICANN, Brazilian President Dilma Rouseff—an outspoken critic of the NSA's mass surveillance programs—announced that Brazil would host an international conference on multistakeholder governance.[4] The conference, titled NETMundial, took place in April 2014 and brought nearly 1500 participants from nearly 100 countries. NETMundial resulted in a proposed set of essential principles for multistakeholder Internet governance and a "roadmap for the future evolution of the Internet Governance Ecosystem."[5] At the meeting, Rouseff also signed the Marco Civil da Internet, the Brazilian Civil Rights Framework for the Internet, into law. The roadmap presented during this meeting in Brazil has since formed the foundation for a range of high-level discussions of the future of Internet governance.

The state of international cooperation on Internet issues is in a state of flux. Many countries are advocating for a stronger role for multi-lateral institutions such as the ITU while others staunchly defend the merits of the multi-stakeholder model. The debates over legitimacy, principle, and practice in the coming year are destined to be impassioned. If the past serves as a reliable guide for the future, we should expect to see a mixture of unilateral, bilateral, and multilateral arrangements cobbled together atop an international network held together by rough consensus and running code. While far from perfect, this ad hoc legal, social, and physical architecture has fared remarkably well.

Notes

1 Sarah St. Vincent, "Coalition Urges Congress to Increase Funding for MLTA Process," Center for Democracy & Technology Blog, November 18, 2014, https://cdt.org/blog/coalition-urges-congress-to-increase-funding-for-mlat-process/.

2 Grant Gross, "U.S. government pulls out of ICANN," PCWorld, March 14, 2014, http://www.pcworld.com/article/2108780/us-government-to-end-formal-relationship-with-icann.html.

3 "Montevideo Statement on the Future of Internet Cooperation," ICANN Announcements, October 7, 2013, https://www.icann.org/news/announcement-2013-10-07-en.

4 "Brazil to host global internet summit in ongoing fight against NSA surveillance," RT, October 10, 2013, http://rt.com/news/brazil-internet-summit-fight-nsa-006/.

5 NETMundial Multistakeholder Statement, April 24, 2014, http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf.

The Rise of Information Sovereignty

Shawn Powers

Many have suggested the Internet's growth means (or should mean) the end of state sovereignty altogether. The logic behind such arguments is compelling. Technology has enabled citizens to create and join communities based not on geography, but on shared interests and ideologies, thus threatening the rationale for state-based nationalism altogether. Why would a citizen pledge loyalty to a state-based nation when a cornucopia of alternative communities that speak to specific interests beckon on the World Wide Web? According to this line of thinking, while states will certainly try to slow the transition, re-asserting their authority and legitimacy, globalization inevitably means the end of the nation-state as we know it.

At the same time, states control the telecommunications infrastructure that enables global connectivity. The physical nature of network connections allows any government to control information flow within its territory in a number of ways, including simply disconnecting its national communications infrastructure from all or parts of the global network. President Hosni Mubarak's decision to take Egypt entirely offline in 2011, as well as Edward Snowden's revelations regarding the existence of government-operated global surveillance apparatus, demonstrate just how vulnerable the web is to state control. Given the ease with which states can control access to the web, what is stopping governments from restricting access to the Internet? After all, even the father of international liberalism—Immanuel Kant—conceded states are motivated first and foremost by self-preservation.[1]

Information sovereignty refers to a state's attempt to control information flows within its territory. But control doesn't necessarily require a government to shut down access to the Internet. It is asserted in a variety of ways, including filtering, monitoring, and structuring industry-government relations in order to maximize state preferences in privately operated communications systems. A 2010 study by the OpenNet Initiative concluded that more than half a billion users—over a third of all users then on the Internet—experienced some form of filtering.[2] This does not include various measures to enforce copyright, prohibitions on hate speech, prohibitions on extremist propaganda, prohibitions on child pornography and exploitation, prohibitions on sales of controlled substances, or prohibitions on online gambling, all of which are enforced by a range of democratically oriented governments.

Monitoring, in particular, is an increasingly powerful means of asserting control over Internet-based communication. As more and more communication moves into the realm of the digital, government capacity to monitor private communication of all types increases. The digitization of information that is central to the Internet's functionality similarly eases government efforts to access, record, and share data from around the world. Drawing on Jeremy Bentham's articulation of the panopticon, Michel Foucault argues that the mere possibility of ubiquitous yet unconfirmed monitoring of a population is among the most effective ways of controlling behavior.[3] As users in Iran and China are well aware, Internet browsing and communication changes drastically when one thinks the government is watching.

Increasingly, both democratic and non-democratic governments are exploring ways to control access

to the Internet without losing legitimacy and, ultimately, power. For some states, access is only restricted in times of emergency, as was the case in Egypt in 2011. For others, access is systematically restricted, as is the case in Iran. China adopts a multifaceted approach, which includes draconian regulation as well as encouraging local, indigenous content creation. The United States is concerned about the consequences of depending on a shared, unsecured Internet, and is thus exploring variety of public-private partnerships in an effort to find the right balance between free speech and security. Denmark, on the other hand, is pioneering the use of digital tools to gain information on potential criminals, as well as cracking down on copyright violations.

Short of permanently cutting off all access to the Internet, governments around the world are exploring the different options for exerting control over domestic information flows. In some cases, these mechanisms allow for greater control over digital communications than was previously asserted over the analogue and interpersonal. Information sovereignty's emphasis on the political rights of governments to control information flows within their geographically delineated territories leverages two simple facts. First, the majority of the world's governments remain eager to protect and strengthen their sovereignty. Second, the majority of citizens support the nation-state system, holding on to nationalist views. As a result, information sovereignty is gaining traction, especially outside the West.

Notes

1 Immanuel Kant, Perpetual Peace, and Other Essays on Politics, History, and Morals, trans. by Ted Humphrey, (Indianapolis: Hackett Publishing Company, 1983).
2 Jillian York, "More Than Half a Billion Internet Users Are Being Filtered Worldwide," OpenNet Initiative, January 19, 2010, https://opennet.net/blog/2010/01/more-half-a-billion-internet-users-are-being-filtered-worldwide.
3 Michel Foucault, Discipline & Punish: The Birth of the Prison (New York: Vintage, 1995).

Boundless Courts and a Borderless Internet

Vivek Krishnamurthy

Ever since Yahoo! sparked a furor in 2004 by disclosing information to the Chinese government about the journalist Shi Tao's email account, which led to his arrest and imprisonment, major Internet companies have structured their operations in a jurisdictionally conscious manner to avoid contributing to human rights violations. Today, Internet companies service customers in some markets from servers located overseas so they can safely ignore requests from authoritarian governments to disclose user data. Similarly, companies often locate key personnel and data centers in jurisdictions with strong protections for civil liberties—in part to signal their compliance with rights-protective laws.

Two recent decisions by courts in established democracies against Internet company operations situated beyond their borders, along with the controversy surrounding the implementation of a third ruling, threaten to disrupt these arrangements, however—with potentially grave consequences for privacy and free expression should other courts adopt their logic.

The first is a decision in April by the federal district court in New York City commanding Microsoft to turn over to federal prosecutors the entire contents of a Hotmail account hosted at the company's Irish data center. Although US laws generally do not apply extraterritorially, the court found that the Stored Communications Act treats emails stored in the cloud as business records belonging to the service provider. As such, customer content stored anywhere in the world is subject to US court orders whenever the service provider operates in the United States. Microsoft is appealing the decision, arguing that the proper way for US law enforcement to obtain access to the Hotmail account is through the Mutual Legal Assistance Treaty with Ireland. Such treaties, which the US has signed with over 60 nations, allows law enforcement in one country to obtain the assistance of the authorities in another to collect evidence, among other forms of cooperation.

In a second case, a court in British Columbia (BC) levied a worldwide injunction in June barring Google from indexing entire domains associated with the sale of counterfeit versions of a company's products. While neither Google nor its Canadian subsidiary have employees or servers in BC, the Court held that it possessed jurisdiction over Google based on its sales of advertising to residents of the province. The Court conceded that most every court around the world would possess jurisdiction over Google on this base, but it nevertheless ruled that it could properly impose a worldwide jurisdiction against Google on the facts of this case, as the aggrieved company and the alleged counterfeiters had closer ties to BC than to any other jurisdiction.

Finally, there is the ongoing controversy over the interpretation of the European Court of Justice's decision in the "right to be forgotten" case, which held that European residents can have "inadequate," "irrelevant," "excessive," or simply outdated information about them de-indexed from search engines. Google in particular has responded to requests to be "forgotten" by de-indexing offending content from its European search offerings, such as Google.de and Google.fr. It has, however, kept such content available on Google.com as well as on its non-European search domains—all of which remain accessible within Europe. These actions have drawn the ire of European privacy regulators, who view

Google's failure to make such content entirely inaccessible in Europe as flouting the decision. No action has yet been taken against Google in this regard, but the possibility of further legal or regulatory action looms.

While courts in established democracies in North America and Western Europe might be trusted to wield extraterritorial powers responsibility, what happens when courts in countries that ignore the rule of law applies these precedents to its own ends? The New York court order to search Microsoft's Irish servers was issued by an impartial judge (mis)construing the rights protections in the U.S. Constitution, but what if a court in, say, Saudi Arabia were to issue a similar order against a company with employees on the ground there for account information stored in the United States? Similarly, what if the courts in Turkey or Thailand were to rule that videos and tweets mocking those countries' heads of states should be banned worldwide, and that they rightfully possess the jurisdiction to do so since their leaders enjoy a closer connection with their home countries than anywhere else? The result would be to reduce content on the Internet to the lowest global common denominator, or to balkanize the Internet into a set of regional networks within which local, rather than international, standards on digital searches and content suppression would prevail.

The current practice of the leading Internet companies to respect assertions of jurisdiction by governments within whose borders particular data is stored, or whose top-level domain graces a particular site, is not a perfect state of affairs. That said, it is far superior to a world in which governments everywhere can make demands of companies anywhere, backed up with the threat of sanctions against employees on the ground if they fail to comply. Regardless of the results in a particular case, courts in the world's established democracies should think carefully about the wisdom of setting precedents that are inherently extraterritorial—given their potential to be abused beyond their national borders.

The Great Firewall Welcomes You!

Nathan Frietas

In the last few years, usage of the mobile messaging app WeChat (微信), developed by Chinese corporation Tencent, has skyrocketed not only inside China, but also around the world. For 500 million mobile users in mainland China, WeChat is one of the only options for mobile messaging available, due to frequent or permanent blockage of apps like WhatsApp, Viber, Line, Twitter, and Facebook. For over 100 million mobile users in the rest of the world, a highly polished user experience, celebrity marketing, and the promise of "free calls and texts" has proven to be nearly irresistible for far-flung members of the Chinese diaspora. This global userbase also includes the Tibetan exile diaspora, who through WeChat have become connected on both sides of the Himalayas in near real-time like never before.

Instead of Chinese users scaling the wall to get out, people around the world are walking up to the front gate, knocking on the door, and asking to be let in. Just as you might expect with a service like WhatsApp or Twitter, every time you send a message on WeChat it is routed through centralized servers, managed by Tencent. In most cases, these servers are located inside of China, often in Shanghai-based data centers, though in some countries, local servers are being set up. These servers, though, are still within reach of Chinese law, regulations, and influence, and all data passing through them is vulnerable to surveillance and censorship.

The first concern is that China's demand for censorship of particular topics and keywords will begin to extend beyond its borders. As detailed analysis from the Citizen Lab's Asia Chats study has shown, censorship keyword lists can vary by geography.[1] If you mention "Occupy Central" in a message sent from WeChat in Beijing to someone in Chengdu, it will likely be blocked and your profile flagged. If you send the same message using WeChat in Toronto to someone in New York, the message will likely go through, though your profile will most likely still be flagged.

The second concern is that communications by a user outside of China, be they a Chinese citizen or not, can be surveilled, logged, and used against them in the future. If you are in San Francisco, and you join a WeChat group chat that is sympathetic to Tibetan self-immolations or the Uighur community, and some members of that group are located in Tibet, Xinjang, and China, then all of your messages and the fact that you are participating in that group chat are communicated to servers managed by Tencent, licensed under the authority of the Chinese government. Since your WeChat account is tied to your real phone number and SIM card, and your full address book is accessible by the app, then your real name and entire community are now flagged as being sympathetic to groups that China considers as harmful as the Islamic State or Al Qaeda. Good luck getting a visa!

The third concern is that this type of service can be used for wholesale extraction of data and insertion of malware into targeted devices. Like most social media apps, the WeChat app on iPhone and Android has full permission to activate microphones and cameras, track your location, access your address book and photos, and copy all of this data at any time to their servers. These types of capabilities are a godsend to attacks known as a RAT (Remote Access Trojan), and usually have to be

snuck onto a laptop through infected PDF files. In the case of WeChat, the user is opting in to these capabilities, entrusting what may be a well-meaning social messaging service with "god mode" while unknowingly providing an easy backdoor on their phone for adversaries higher up the Chinese cyber-war food chain.

Illustration by Willow Brugh

Combined with the rise of attractive, low-cost mobile handsets from Huawei and Xiaomi that include China-based cloud services, which are being sold in India and elsewhere, the world is witnessing a massive expansion of Chinese telecommunications reach and influence, powered entirely by users choosing to participate in it. The fundamental question is: do the Chinese companies behind these services have any market incentive or legal obligation to protect the privacy of their non-Chinese global userbase? Do they willingly or automatically turn over all data to the Ministry of Public Security or State Internet Information Office? Will we soon see foreign users targeted or prosecuted due to "private" data shared on WeChat? Finally, from the Glass Houses Department, is there any fundamental difference in the impact on privacy freedom for an American citizen using WeChat versus a Chinese citizen using WhatsApp or Google?

For those of us in the global community who care both about ensuring that all humans can be more interconnected and provided free, unlimited access to knowledge, while also ensuring their privacy and dignity is protected, these are primary issues we must study, understand, and take action on. The next 5 billion people on Earth tend to live in more repressive places than free ones, and we must ensure that their desire to be connected in a "free and unlimited way" does not leave them in a virtual panopticon.

Notes

1 Citizen Lab, "Asia Chats: Analyzing Information Controls and Privacy in Asian Messaging Applications," November 14, 2013, https://citizenlab.org/2013/11/asia-chats-analyzing-information-controls-privacy-asian-messaging-applications/.

Toward an Enhanced Role of Academia in the Debates About the Future of Internet Governance—From Vision To Practice

Urs Gasser

Academics, academic institutions, and academic values have played a key role in the development of the Internet as well as in its operation and in what we today call "governance," especially at the logical layer consisting of technical standards and protocols. Indeed, it is impossible to imagine the Internet as we know it without the defining role academics have played since its inception in the 1970s. Similarly, core academic values such as openness, collaboration, and trust have inspired the early approaches to and initial modes of Internet governance, and have shaped its evolution since the 1990s. Important traces of these academic origins are still reflected in today's multi-stakeholder Internet governance ecosystem, which has come under significant pressure since the World Summit on the Information Society (WSIS)[1] in 2003 and 2005 and, perhaps most visibly, at the 2012 World Conference on International Telecommunications (WCIT-12).[2]

The contested policy debates that currently take place across various national and international forums—from NETmundial[3] to the ITU's 2014 Plenipotentiary Conference[4] and WSIS+10,[5] to name just a few—suggest that we have arrived at crossroads in the debates about the future of Internet governance. In the light of today's heated debates, this essay argues that it is timely to reflect on academia's role in the development and operation of the Internet over the past two decades and to renew its commitment to contribute systematically and from diverse perspectives to the Internet governance debates over the next decade. Second, it proposes an enhanced role of academia as we design the next-generation Internet governance model—a role that builds upon past contributions but is also based on a generalized vision and strategy regarding the importance of academic research, facilitation, experimentation, and education. Such an enhanced role emphasizes academic values such as independence, rigor, openness, and global participation. Before outlining the contours of an enhanced role of academia, let us turn to the question: why we should re-imagine the role of academia, and why now? The short answer is: because there is critical need, and because there are opportunities we should embrace.

Since the early days of the Internet governance, the world has changed dramatically, and so has the academic environment. When ICANN was founded in the late 1990s with the help of researchers at the Berkman Center, for instance, only a handful of academics were researching Internet and society issues. Today, Internet studies—or Internet science, as it is labeled in Europe—has evolved from an academic niche area (typically researched at law schools, given the porous methodological boundaries of law as a discipline) into an academic discipline in its own right, with emerging research methods, specialized journals, degree programs, chairs, and centers. We see more and more young people—master students, doctoral students, and so forth—interested in this growing field of research and work, most of whom share a strong interest in and commitment to interdisciplinarity. Similarly, it is no longer the stereotypical group of "white males in their 60s" actively addressing Internet governance issues, broadly defined, but an increasingly diverse community of scholars, researchers, and activists—many of them talented women and young people from the Global South. This generational shift, the increased diversity in terms of gender, orientation, and geographic representation, the com-

mitment to interdisciplinary, and novel institutional support structures provide a unique opportunity for coordinated and sustained academic collaboration on issues related to Internet governance that we should harness, adding perspectives from other domains, incubating alternative approaches and models, and re-energizing the great work previous generations of academics have contributed.

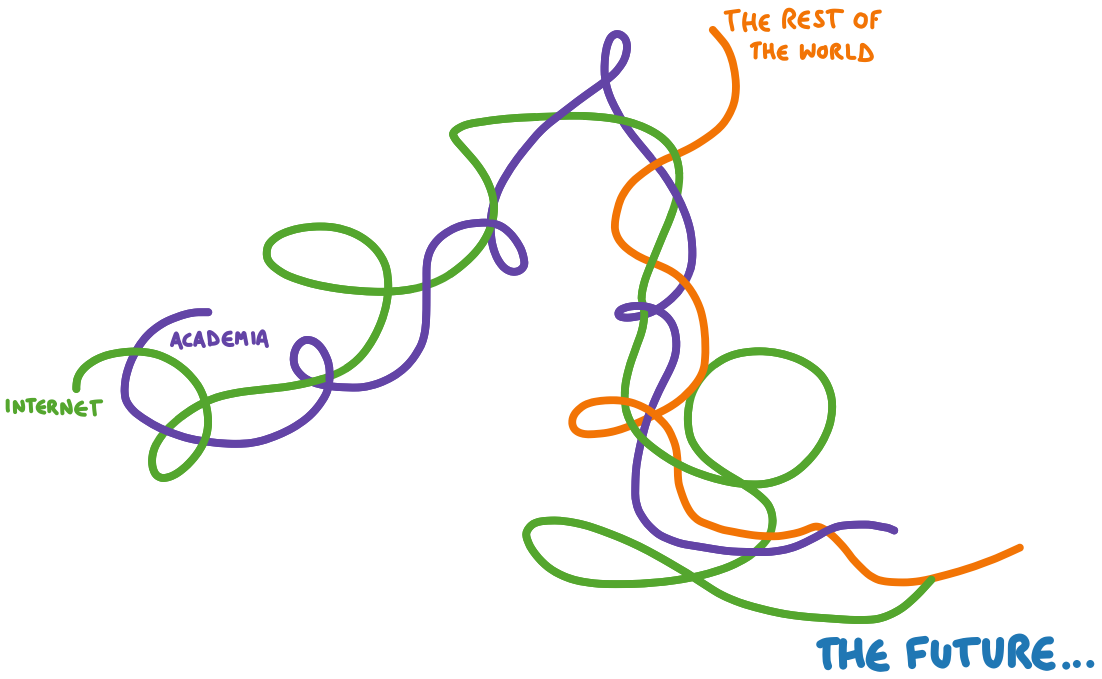


Illustration by Willow Brugh

It is not only opportunity, but also increased and pressing need that calls for a renewed commitment of academia based on a broader vision and strategy concerning its future role in the global debates about the future of Internet governance. It is commonly understood that the Internet now affects almost every aspect of life, that its governance has become more complex, and that the stakes are much higher than they were two decades ago. Controversies about multilateral versus multi-stakeholder approaches to Internet governance as well as the battles over a diverse set of issues (ranging from surveillance to intellectual property) are manifestations of the importance of the Internet as the core information and communication infrastructure of the digital age. In such a contested and highly politicized environment, it is vital to build upon, expand, and accelerate past academic efforts by broadening and coordinating the scope of inquiry, working towards institutional approaches, and developing global capacity. There is an increasing demand across all stakeholders for independent and rigorous research and scientific data, as well as for best practices and general principles that are created collaboratively and in the spirit of the academic values mentioned before. Viewed from such a perspective, academia can and should be more than a "stakeholder" in today's Internet governance debates. It is well-positioned to play a constitutive role as we develop a new vision of a next-generation Internet governance ecosystem in a time when governance debates are often ideological, fragmented, and mostly interest-driven rather than evidence-based.

At this critical juncture and in the light of new opportunities and pressing demands related to Internet governance, what could an enhanced role of academia look like in practice? A concrete example and

precursor in this context is a recent initiative by the Global Network of Internet & Society Research Centers,[6] which was incubated by the Berkman Center, built bottom-up, based on international collaborations, and formally launched in 2012. It now brings together more than 30 academic centers[7] with focus on Internet and society issues from around the globe, including nine members from the Global South. The network represents a broad range of disciplines, bridges many traditions and cultures, and engages many young as academics from diverse geographic backgrounds. As an evolving and learning network, it represents some of the key elements of the enhanced vision mentioned before, including the emphasis on institutional approaches and global capacity development, interdisciplinary research and building, systematic and sustainable engagement, and the engagement of new perspectives and talents.

In addition to these structural elements, an enhanced role of academia also calls for a concerted and sustained thematic engagement across the various layers of Internet governance research. Consider the following three questions as an illustration of the breadth of the issues that need to be addressed on different layers (others could be added):

- Data and research layer: What can we do, as a network of academic institutions, to create a global interoperable data platform to measure the Internet's health, which could serve as an information backbone for Internet governance research and decision making, providing high quality and open data to distributed Internet governance groups?
- Normative layer: How can academia serve as a "protected space" to develop the necessary normative foundations of future Internet governance models and mechanisms and facilitate difficult value conversations among Internet governance stakeholders, working towards consensus, good practices, and general principles of Internet governance?
- Design layer: Building upon research activities and conceptual studies, how can we as an academic community work together—in interdisciplinary teams and across departments, schools, and centers—to develop new institutional designs, experiment with new tools, and create new code or Internet governance?

These three examples indicate not only the broad range of possible contributions, which together with other elements might serve as the foundation of a holistic concept of Internet governance, but also point to the different modes of academic engagement in the multi-faceted Internet governance processes. The envisioned core pillars to which the examples partly allude, but need to be fleshed out elsewhere, include research, facilitation, experimentation, and education (encompassing also skill building and practical training).

The partnership between the Berkman Center and the Network of Centers and the engagement of this institutional network in the current discussions about the future of Internet governance through a coordinated events series[8] and a research pilot[9] are intended as an initial step towards operationalization of the broader strategy and underlying vision as sketched in this essay. The Network of Center's research pilot consists of a case study series as building blocks of a synthesis document aimed at deepening our understanding of the formation, operation, and effectiveness of distributed Internet governance groups. The research examines a geographically and topically diverse set of local,

national, and international distributed governance models, components, and mechanisms from within and outside the sphere of Internet governance. With its initial focus on emerging lessons learned and (contextual) good/best practices, the goal of the research pilot is to inform the evolution of the Internet governance ecosystem in the light of the NETmundial Principles and Roadmap, the discussions at the Internet Governance Forum (IGF), and other forums, panels, committees, and initiatives.

In parallel to weighing in on these and related conversations about the next-generation Internet governance models and mechanisms, academia has a responsibility to re-envision its own future in this zone, reflecting and building upon the great contributions of the past. The months and year to come will provide a unique window of opportunity to further flesh out the proposed vision and strategy for an enhanced role of academia, incorporating lessons learned from current efforts and pilots. Contributions by the Network of Centers, as well as related efforts such as the Global Internet Governance Academic Network (GigaNet[10]) and the Research Advisory Network (RAN) to the Global Commission on Internet Governance, are important building blocks in this respect. But working from vision to practice will require not only collaboration among academic networks around the globe. Success will also depend on longer-term commitments by leaders in the public and private sector as well as open participation of civil society actors. Realizing the promise of an enhanced role of academia is a shared responsibility as we build together an Internet governance system for future generations.

Additional Reading

DeNardis, Laura. The Global War for Internet Governance (New Haven: Yale University Press, 2014).

DeNardis, Laura, and Mark Raymond. "Thinking Clearly About Multistakeholder Internet Governance," SSRN, November 14, 2013, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2354377.

"Developing Meaningful Multistakeholder Participation Mechanisms," IGF 2014 Best Practices, Internet Governance Forum, 2014, http://review.intgovforum.org/igf2014/best-practices/developing-meaningful-multistakeholder-participation-mechanisms/.

Drake, Bill, and Monroe Price, eds.. Beyond Netmundial, August 2014, http://www.global.asc.upenn.edu/app/uploads/2014/08/BeyondNETmundial_FINAL.pdf.

Dutton, William H., ed. The Oxford Handbook of Internet Studies (Oxford: Oxford University Press, 2013).

Leiner, Barry M., Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, and Stephen Wolff. Brief History of the Internet, http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet.

Mueller, Milton. Networks and States: The Global Politics of Internet Governance (Cambridge: The MIT Press, 2010).

"NETmundial Multistakeholder Statement." Global Multistakeholder Meeting on the Future of Internet Governance, Rio De Janeiro, Brazil, April 24, 2014, http://netmundial.br/netmundial-multistakeholder-statement/.

Palfrey, John, and Jonathan Zittrain. "Better Data for a Better Internet," Science 2 December 2011, Vol. 334 no. 6060 pp. 1210-1211, http://www.sciencemag.org/content/334/6060/1210.full?ijkey=yLssWDbbr0ekI&keytype=ref&siteid=sci%2520.

Radu, Roxana, Jean-Marie Chenou, Rolf H. Weber, eds.. The Evolution of Global Internet Governance. Principles and Policies in the Making (Berlin: Springer, 2013).

Waz, Joe, and Phil Weiser. "Internet Governance: The Role of Multistakeholder Organizations". Journal on Telecommunications & High Technology Law, 10, (2012): 331, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2195167.

Weber, Rolf H. Regulatory Models for the Online World (Berlin: Springer, 2002).

---. Shaping Internet Governance: Regulatory Challenges (Berlin: Springer, 2009).

Notes

1 World Summit on the Information Society, http://www.itu.int/wsis/index.html.
2 2012 World Conference on International Telecommunications, http://www.itu.int/en/wcit-12/Pages/default.aspx.
3 NETmundial, http://netmundial.br/.
4 ITU Plenipotentiary Conference 2014, https://www.itu.int/en/plenipotentiary/2.
5 WSIS+10, http://www.itu.int/wsis/review/2014.html.
6 Global Network of Internet & Society Research Centers, http://networkofcenters.net/.
7 "Participating Centers," Global Network of Internet & Society Research Centers, http://networkofcenters.net/centers.
8 "Events," Global Network of Internet & Society Research Centers, http://networkofcenters.net/events.
9 "Research," Global Network of Internet & Society Research Centers, http://networkofcenters.net/research.
10 GigaNet, http://giga-net.org/.

Proliferation of "Internet Governance"

Rolf H. Weber

According to a well-known description, Internet Governance "is the simplest, most direct, and inclusive label for the ongoing set of disputes and deliberations over how the Internet is coordinated, managed, and shaped to reflect policies."[1] In other words, Internet Governance "evolves" the design and administration of the technologies necessary to keep the Internet operational and facilitate the enactment of substantive policies around these technologies.[2] Such design requires the fructification of law as instrument structuring an order in the public interest.

1. Functions of law

The functions of law crystallize in a system of rules and institutions that underpin civil society, that facilitate orderly interaction, and that resolve disputes and conflicts arising in spite of such rules. Law can be created by way of negotiation, imposition, and evolution. In cyberspace, the evolutionary aspect is of major importance since new concepts are developing, for example through the creation of normative principles or the implementation of "rules" derived from codes of conduct, corporate social responsibility, and other similar initiatives.

Law is able to regulate behavior, and it allows people in a community to determine the limits of what can and cannot be done in their collective interest. Law as a structural system is traditionally featured with coercive effect.[3] If law is properly implemented, its provisions can be enforced against the will of individuals. However, irrespective of its (coercive) quality, the legal system is embedded in other socially relevant systems; in particular, "cyber-norms" depend on social norms.[4] Developments in technology and/or society, expressed in informal standards, can and should give input to legislative bodies; thereby, the acceptability of legal norms increases if they are based on informal social standards that are derived from customary behavior of civil society.[5]

The relativity of norms reflecting civil society's needs is evidenced by the fact that norms can come in a variety of shapes with different effects; insofar the legal system is linked to other social sub-systems and executed through a framework of structural couplings.[6] Such kind of structure calls for a multilayered approach in norm-setting.[7]

When designing the future cyberspace legal framework[8] the fact should be considered that architects are the experts in sketching "constructions." More than a hundred years ago, the famous architect Louis H. Sullivan said: "It is the pervading law of all things, organic and inorganic, of all things, physical and metaphysical, of all things human and all things superhuman, of all true manifestations of the head, of the heart, of the soul that the life is recognizable in its expression, that form ever follows function. This is the law."

Sullivan uses the word "law" twice while attributing the notion of making form dependent on function. Therefore, when designing a global Internet Governance framework, the function of law has to be considered in more depth; following Bentham's principle of utility and Luhmann's approach of

stabilization of normative expectations, a functional approach that bodes for the political design of Internet Governance should determine the normative order.

As a result, the main question could be phrased as follows: What social impacts should be caused by law? The answer is based on the expectations of civil society. These expectations change over time, but some elements remain the same, such as legal certainty, stability, and reliability. In times of fast developing information technologies, civil society is better able to rely on these principles in an informal law-making process and context than in the traditional legal regime.
Thesis 1: A functional approach of rule making is necessary to adequately capture socio-political expectations of civil society.

2. Increased dynamics through socio-technological developments

Technological developments in the information and communication field, particularly the process of digitization, have caused advances that lead to widespread social change.[9] These advances need to comply with at least three social expectations:[10] (i) applications for the public have to be available from a technical point of view; (ii) applications and projects leading to them must be socially and commercially acceptable; and (iii) the implementation and usage of the systems should be done such that they are achievable from a cultural perspective.

In the Internet context, technological developments require an adaptation of the regulatory design and its modalities, which can be differentiated into socially-mediated modalities and environmental modalities. Thereby, the regulatory authority called upon to settle a regulatory disruption may choose to "utilize any of the socially mediated modalities either alone or in a hybrid regulatory model."[11] Correspondingly, modern socio-legal theory has tried to develop models that ideally should overcome legal instability. As a consequence, the legal framework should encompass the socially desirable requirement that netizens be members of civil society and should simultaneously become manageable, available, realistic, workable, and interwoven easily with all aspects of social life.

These developments caused by technologies and influencing the social/environmental parameters of an open society make the regulatory systems more dynamic. Cyber-communities are successfully able to shape their internal relations with non-legal tools (technical standards, terms of use, codes' of ethics).[12] Therefore, regulators have to take into account the assessments of network engineers and communication theorists pointing to the vital function played by environmental layers in communications networks even if such approach leads to a complex structural matrix.[13]

Scholars have tried to capture these increased dynamics with a "global experimentalist governance" theory ("GXG"). An ideal GXG regime comprises five key steps,[14] namely: 1) initial reflection and discussion among stakeholders; 2) articulation of a framework understanding with open-ended goals; 3) implementation of these broadly framed goals; 4) continuous feedback provided from local contexts; and 5) periodic and routine re-evaluation of the goals and practices (including their possible adaption or revision). Certain similarities of the GXG approach with the multi-layer or network governance model do exist; however, GXG puts more emphasis on new forms of learning. A condition for GXG is

that States are unable to formulate a comprehensive set of rules and effectively monitor compliance. Furthermore, States must not be stymied by disagreement over basic principles, and the cooperation of civil society actors either as agenda setters or as problem solvers is normally indispensable. A problem with the GXG approach exists in its vulnerability to manipulation and unintended consequences, even if GXG has the potential to increase participation in, and thus the democratic legitimacy of, institutions. Additionally, the foreseeability and the predictability of legal norms are low, and a link to the international legal setting is missing.

Thesis 2: A stable Internet Governance framework can only be established if the respective rules reflect the socially desirable and manageable requirements of the civil society's members.

3. Rule making in favor of open society

The technological and social developments also contribute to the establishment of an "open society."[15] The aims of this openness—evolving in a perpetual process of attempts to ameliorate and correct errors—are the preservation of individual freedom as well as the ideal of political-ideological pluralism. Openness and acceptance of other approaches and solutions for problems should be available, leading to a comparative environment and allowing the best alternative to establish itself.[16] Cyberspace is particularly apt for an "open society," since new possibilities for participation may be discovered and previous involvement processes could be ameliorated.

The "openness" also presupposes that public forums are accessible and allow an exchange of opinions. This transparent scheme would allow widespread involvement of participants with different backgrounds and manifold ideas; taking note of other individuals' opinions can lead to dynamic processes being directed to new social and environmental horizons.[17] This kind of involvement is particularly important, since behind every new technology lurks someone's desire to exert control over it.[18]

Networks can be characterized as systems partly overlapping and, therefore, requiring "bridges"; freedom and power are affected by the degree of openness, i.e. by the extent "to which individuals can bob and weave between networks to achieve their designed behavior, actions/perceptions, or outcomes."[19] The relation between the freedom and the aforementioned three appearances of human activities can be deepened and combined in complex configurations depending on the democratizing environment. In preparing norms it is important to understand the level of freedom and its sources, thereby enabling the rule makers to design a structure that leads to an appropriate equilibrium between the diverging interests.

Nowadays, the openness of cyberspace is threatened by governmental and private control regimes: the security-industrial complex applying extensive surveillance measures—including by co-opting private actors—has significant potential in the hand of dictatorial regimes; its technologies of control and lobbying power, mostly obscured from public gaze, might increase over the coming decade and thereby cause serious threats to individual human freedoms in cyberspace.[20]

From the private side, the openness of cyberspace can be endangered by cryptographic means (for

example encrypted songs or movies) and the implementation of the digital rights management by rightsholders. Furthermore, openness must be ensured on the private side by restricting dominant stakeholders from blocking rival content threatening their own commercial interests (for example by transforming open platforms into "walled gardens").[21] A vigorous enforcement of the openness rules in order to maintain access to innovation is needed in times of increasing establishment of horizontal and vertical bottlenecks to distribution.

Recently, the inventor of the World Wide Web, Tim Berners-Lee, proposed to implement a "Magna Carta" in order to protect and enshrine the independence of cyberspace. The web he created 15 years ago has come under increasing attack from governments and corporate influence, making it necessary to ensure an "open, neutral" system. Berners-Lee's Magna Carta plan is supposed to be taken up as part of an initiative called "the Web we Want," which calls on people to generate a digital bill of rights and an open Internet.

Openness of cyberspace corresponds to the principle that the Internet must be seen as a public sphere encompassing multiple publics with manifold interests.[22] From this perspective, openness is also a prerequisite for combatting the fragmentation of network structures. As outlined by the European Commission, the vision for cyberspace governance must consist of a single, un-fragmented network.[23]

Thesis 3: A key objective of Internet Governance should consist of the permanent promotion of openness constituting a universal concept that enshrines free access and free communications' principles.

4. Appropriateness of multi-layer structure

In the cyberspace context, different layers have to design the framework of regulations: the basic differentiation necessary in the design concerns the facts and values of the underlying reality; this assessment leads to the distinction of descriptive and evaluative elements on the level of social norms (informal normative order) and legal norms (institutional normative order).

Multi-layer governance requires the development of common foundations applicable to all relevant layers; at the same time, it must respect diversity and pluralism in order to be commensurate with the respective level of integration. An important aspect of this movement is the acknowledgment of the need for increased cooperation when trying to achieve a multi-layer consistency.

Multi-layer governance addresses normative guidance as to how relations between different layers of governance should be framed in a coherent manner, encompassing both analytical and prospective issues in building upon observations of legal phenomena. The definition of the proper interaction of the different levels has a direct impact on an ideally coherent regulatory architecture of multi-layer governance, i.e., multi-layer governance "proposes a process and direction."[24] If common legal rights and obligations can be identified, the ensuing legal framework enjoys special legitimacy, which is essential for the operation and effectiveness of law.[25]

Since regulatory frameworks evolve within a given societal and political context, private regimes are part of the overall legal design, particularly if their weaknesses can be eliminated or at least diminished. These regimes have a certain place in a multi-layer structure, if developed with the objective of establishing an appropriate institutionalization, based on broad initiation and wide building support. Other elements are the significance of the institutional environments, the dynamics of relationships, and how non-sovereign bodies respond to multiple legitimacy claims in complex and dynamic regulatory situations. In relation to non-state or private networks and organizations, the governance emphasis should not be based on normative validity; moreover, the trend towards efficiency and public value maximization also needs to be supported.

Notwithstanding the fact that some elements that define multi-layer governance in a global context seem diffuse, important core themes can be extracted:[26]

- Future regulatory problems by their nature will require broader and more collective decision making than applied in traditional regimes; global interactions necessitate the establishment of a multistakeholder regime.
- Responses to new problems are complex on the global level, and flat structures on different sub-levels facilitate decision making by including the relevant persons and organizations in the process at the actual point of their respective concern.
- The ongoing processes of globalization and integration necessarily lead to an altered perception and notion of State sovereignty and ask for new elements of legitimacy in this respect.

The described multi-layer concept also goes hand in hand with the increasingly prevailing multistakeholder approach to Internet Governance.

Thesis 4: Multi-layer governance is necessary in order to enshrine descriptive and normative elements into the decision-building processes and to lay the ground for the realization of the multistakeholder approach.

5. Improved quality of rule making

In view of these developments, the conditions for regulatory quality and performance must be designed in a way that both socially mediated and environmental modalities can be adequately taken into account. The realization of these objectives calls for the implementation of the multi-layered concept; a proper interaction of the different levels has a direct impact on an ideally coherent regulatory architecture.

Irrespective of the implemented substantive legal principles for cyberspace, however, it is necessary to ensure that the norm setting reaches an adequate level of quality. A consensus of all concerned cyberspace actors on the rule-making body does not suffice if the norms are so defective that they do not achieve the envisaged normative objectives. Three problems are particularly noteworthy in this context:[27]

- In developing new norms, rule makers have to avoid creating conflicts with other rules that are already part of the cyberspace users' law system. Therefore, rule makers should research the norms of the concerned community and only then define the new rules that fit into the existing framework. Depending on the given circumstances, new rules may be able to modify existing norms by gradually extending their scope into the rule makers' desired direction, if this direction is not irreconcilable with the existing framework.
- Another problem consists of the concrete drafting of new rules; if cyberspace actors do not understand the wording, compliance with the rules can hardly be expected or achieved. In other words, the linguistic quality of norms is of importance; insufficient quality is a widely known issue in rule-making processes. In addition, if new rules do not take up the requirements of the socio-technological environment, obedience by cyberspace actors is not facilitated.
- A third pitfall occurs if the law is framed in terms that have no apparent connection to what the cyberspace actors actually do. If the relationship between the demands of the rule maker and the behavior of cyberspace actors is not recognizable, rejection and non-compliance by cyberspace actors are likely, since the respective new rule does not appear to be established on the basis of a meaningful concept. Only meaningful and respectful laws will not encounter resistance from the addressees of the norms (i.e., civil society).

As known from general law-making theories, an appropriate trade-off between simplicity and certainty with respect to the application of new rules is difficult to achieve; as a consequence, rule makers have to carefully assess cyberspace actors' required intentions, behaviors, and outcomes in some detail. As mentioned, another general observation consists of the acknowledgement that law should be embedded in a social concept and that law can hardly operate as a mechanism for controlling the behavior of cyberspace actors. Therefore, the purpose of a rule-making process should be to regulate functions and effects, not means.

Thesis 5: Rule-making bodies should strengthen the efforts to improve the quality of regulation in order to comply with the requirements of a legal framework that meets the needs of civil society.

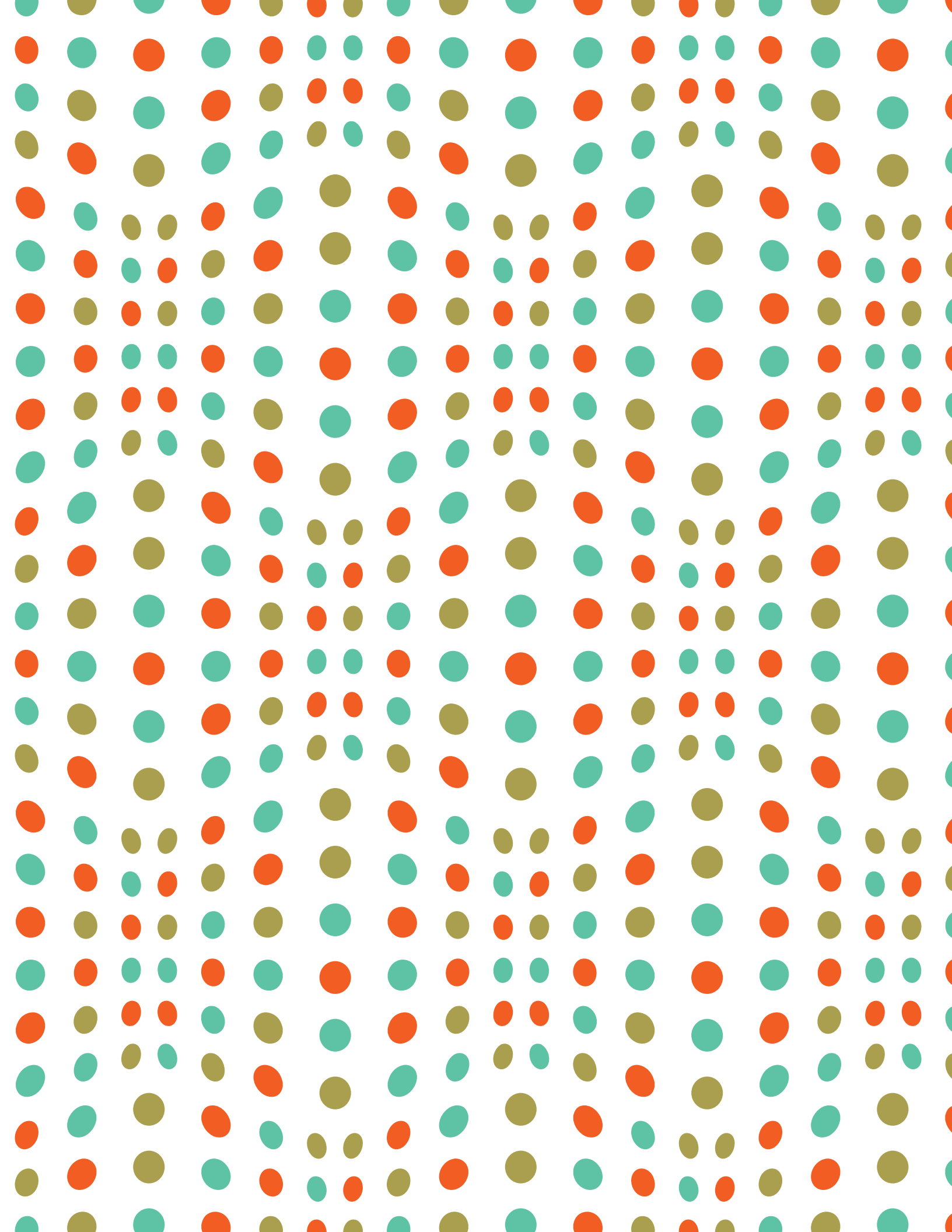
6. Outlook

The concept of multi-layered governance requires common foundations applicable to all relevant layers, while at the same time it must respect diversity and pluralism by developing normative guidance as to how relations between different layers of governance should be framed in a coherent manner. Consequently, Internet Governance advocates should enlarge the interdisciplinary scope of thinking by taking into account the multi-layered regime in the further proliferation of regulatory concepts.

Notwithstanding the different perceptions of the various stakeholders in cyberspace, the principles agreed upon in the manifold fora need to be embedded into a comprehensible structure. This objective can be achieved if—apart from the technical operability—the legal interoperability is also improved. Legal interoperability is the process of making legal rules work together across jurisdictions. Whether new laws are implemented or existing laws are adjusted or reinterpreted depends on the given circumstances. In view of the increasing fragmentation of cyberspace regulation, efforts should be undertaken to achieve higher levels of legal and policy interoperability in order to reduce costs in cross-border business and to drive innovation and economic growth.[28]

Notes

1 Milton Mueller, Networks and States. The Global Politics of Internet Governance (Cambridge: The MIT Press, 2010), 9.
2 Laura DeNardis, The Global War for Internet Governance (New Haven/London: Yale University Press, 2014), 6.
3 Herbert L.A. Hart, The Concept of Law, 2nd ed. (Oxford: Oxford University Press, 1997), 55-57.
4 April Mara Major, "Norm Origin and Development in Cyberspace: Models of Cybernorm Evolution," Washington University Law Quarterly 78 (2000), 59-111, 86.
5 Rolf H. Weber, Regulatory Models for the Online World (Zürich: Springer, 2002), 32.
6 Niklas Luhmann, Das Recht der Gesellschaft (Frankfurt: Suhrkamp Verlag, 1993), 93, 187-191, 441.
7 Rolf H. Weber, "Multilayered Governance in International Financial Regulation and Supervision," Journal of International Economic Law 13 (2010), 683-704.
8 Louis H. Sullivan, "The tall office building artistically considered," Lippincott's Magazine 57, March 1896, 403-409, reproduced in: Leland M. Roth (ed.), America builds: Source Documents in American Architecture and Planning (New York: Harper Collins, 1983), 340-345, 345.
9 Andrew D. Murray, The Regulation of Cyberspace: Control in the Online Environment (Milton Park: Routledge-Cavendish, 2007), 30-35.
10 Richard Susskind, The Future of Law (Oxford: Oxford University Press, 1996), 240.
11 See Murray (supra note 9), 40.
12 Joanna Kulesza and Roy Balleste, "Science and Importance in Cyberspace: The Rise of Use Internet as a New Order in International Law," Fordham Intellectual Property, Media & Entertainment Law Journal 23 (2013), 1311-1349, 1346.
13 See Murray (supra note 9), 43.
14 See Gráinne de Búrca, Robert O. Keohane, and Charles F. Sabel, "Global Experimentalist Governance," British Journal of Political Science 2014 (forthcoming), now available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2423810.
15 Karl Popper, The Open Society and Its Enemies, (London: Princeton University Press, 1945).
16 Rolf H. Weber and Romana Weber, "Social Contract for the Internet Community? Historical and Philosophical Theories as Basis for the Inclusion of Civil Society in Internet Governance?," SCRIPT-ed 6 (2009), 90-105, 96.
17 See Weber and Weber (supra note 16), 96.
18 See Kulesza and Balleste (supra note 12), 1313.
19 Yochai Benkler, "Network Theory: Networks of Power, Degrees of Freedom," International Journal of Communication 5 (2011), 721-755.
20 Ian Brown and Christopher T. Marsden, Regulating Code: Good Governance and Better Regulation in the Information Age (Cambridge: The MIT Press, 2013), 162.
21 Salil K. Mehra, "Paradise is a walled garden? Trust, antitrust and user dynamism," George Mason Law Review 18 (2011), 889-952.
22 Rikke Frank Jørgensen, Framing the Net: The Internet and Human Rights (Cheltenham: Edward Elgar Publishing, 2013).
23 European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "Internet Policy and Governance: Europe's role in shaping the future of Internet Governance," COM(2014) 72 final, February 12, 2014, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52014DC0072.
24 Thomas Cottier, "Multilayered Governance, Pluralism, and Moral Conflict," Indiana Journal of Global Legal Studies 16 (2009), 647-679, 656.
25 Weber (supra note 7), 690.
26 See Rolf H. Weber, Shaping Internet Governance: Regulatory Challenges, (Zürich: Springer, 2009).
27 See Chris Reed, Making Laws for Cyberspace (Oxford: Oxford University Press, 2012), 226-228.
28 John Palfrey and Urs Gasser, Interop: The Promise and Perils of Highly Interconnected Systems (New York: Basic Books, 2012), 177-179.



LOOKING FORWARD

Robert Faris

In surveying the global digital landscape, several starkly different realities are evident, each with its own set of priorities and problems. For much of the world's population, simply getting online is the most pressing issue of the day. A major concern is that the lack of adequate Internet infrastructure represents a major impediment to cultivating the capacity to more fully participate in the 21st century global economy, and that the current digital divide constitutes an additional and persistent wedge between the fortunes of the developed and developing world. This gap extends beyond physical infrastructure; differences in both digital literacy and agency also pose obstacles to online engagement. Questions for the coming years include how well the combination of public and private investments in infrastructure, national broadband policies, technological advancement, and education can help to bridge this gap, and what the long-term costs will be for those countries that do not.

For netizens that reside in well-connected countries with restrictive online environments, the infringement on political and civic liberties is a persistent issue with direct and indirect implications on social and economic development. In addition to the acute human rights problems, a point of central concern is that these restrictions inhibit the development of civil society institutions and social capital that are essential building blocks for modern societies to flourish. Yet identifying the most likely paths toward greater liberalization of digital spaces in autocratic regimes remains elusive. The development and dissemination of tools that help users circumvent content filters, protect Internet resources from cyberattacks, and aid in maintaining anonymity online help to create an environment for the politically active in authoritarian regimes where they can more freely express and share ideas. It is less clear how this technologically driven and limited opening of Internet spaces contributes in the long term to the reform of policies and regulations to protect Internet openness.

A particular concern is that more countries will choose to take steps to further wall themselves off from the open Internet. A question for the coming year is whether Russia will enforce proposed data localization policies, and if they do, how international social media and technology companies will respond. There appears to be a real risk that Russia will create a domestically hosted Internet enclave similar to that found in China, which would allow the government, should it decide to do so, to bring restrictions on digital media even closer in line to the controls on broadcast and print media. A related question is how many other countries, if able to do so, would apply a Chinese-style censorship regime: dialing up and down controls on political speech while allowing Internet activity to thrive in other areas. Iran is an example of a country that has failed to create such an environment and instead has opted for crippling restrictions on Internet activity, although if ongoing attempts to add further controls are telling, has also failed to impose the political control it seeks.

In those countries that show greater respect for freedom of expression and civil liberties online, the regulatory fabric includes a mix of private ordering, formal legal obligations, and informal arrangements with companies and regulators, alongside surreptitious activity, much of which is illegal. There are several trends that bear watching.

There appears to be growing support for clearly and proactively delineating Internet rights. This trend got a large boost from Brazil when the legislature there passed the Marco Civil da Internet. It will be

interesting to see how many other countries enact similar frameworks. Efforts to codify Internet rights are underway in Italy and France, and appear to be indicative of a larger trend informed by more than 70 different proposals for defining fundamental rights online.

The mechanisms and structures for coordinating Internet governance internationally may undergo significant changes in the coming year. Several forums are studying and discussing how to best forge global consensus on matters related to Internet governance and how the various multistakeholder and multi-lateral approaches can best contribute to global coordination.

Another complex and important set of questions are teed up for countries that are committed to protecting free speech but also seek to address incursions into privacy and lessen the harms to citizens through damaging online activity, such as defamation, harassment, misogyny, racism, threats of violence, and other malicious attacks. Just as the efforts to protect Internet rights may be contagious, the policies and mechanisms used to curtail speech will be copied and emulated. Strategies to enforce a right to be forgotten online are from one perspective well justified and from another perspective deeply flawed in their implementation. The search for and debate over alternative mechanisms to achieve similar results is underway and may influence the spread of such policies. A similar set of trade-offs will complicate any initiative to more aggressively police extremism online.

Another issue to watch in the coming months and years is the many efforts to encrypt personal communications. Many people are working on this issue with renewed vigor, and an increasing number of companies appear to view this issue as an important factor in their competitive standing. The willingness of companies to be more aggressive in building encryption into their services as a default option will have the biggest impact on the speed and reach of diffusion. The response by law enforcement agencies will also be interesting as they continue to take the argument that they been honing for many years—that unimpeded access to digital communication is essential for protecting the public from crime and terrorism—to political leaders and the general public.

CONTRIBUTORS

Ana Azurmendi is a Professor of Media Law at the Faculty of Communication, University of Navarra (Spain). She was previously an Appointed Professor at the Doctoral Program on Human Rights, University of Salamanca-Panamericana University; at the Comparative Media Law Program, University of Oxford; and at the Faculty of Law, University of Paris II (2003), Program "Droit Approfondi des Mèdias." She is the author of several books, including Derecho de la Comunicación (Communication Law), La Reforma de la Televisión Pública Española (Spanish Public Television Reform), and El derecho a la propia imagen (The Right to Self Image).

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.

Susan Benesch founded the Dangerous Speech Project to find ways of diminishing inflammatory speech—and its capacity to inspire violence—while protecting freedom of expression. She has developed a framework to estimate the dangerousness of speech in context, and has tested ways to help audiences to resist dangerous speech, especially in Kenya. As a Faculty Associate at the Berkman Center for Internet & Society, she is carrying out a new project to test the effectiveness of anti-hatred efforts online. Using the results, she hopes to design new, more effective methods to diminish online hatred and inflammatory speech.

Eduardo Bertoni is the Director of the Center for Studies on Freedom of Expression and Access to Information (CELE) at the Universidad de Palermo. Previously, he was the Executive Director of the Due Process of Law Foundation (DPLF) and the Special Rapporteur for Freedom of Expression of the Inter-American Commission of Human Rights at the Organization of American States.

Ellery Roberts Biddle is a writer, editor, and advocate for the protection of human rights as they exist on the global Internet. She is the editor of Global Voices Advox, a network of bloggers and advocates dedicated to reporting on threats to online speech, sharing tactics for defending the digital work and words of citizens, and supporting efforts to strengthen Internet policy and practice worldwide. She is also a Fellow at the Berkman Center for Internet & Society.

Willow Brugh is an organic chat client, spanning a multitude of subcultures and putting like-minded (but differently disciplined) people in touch. Many of these connections are made at events Brugh co-organizes and facilitates like Random Hacks of Kindness, SpaceApps Challenge, Konbit Technologie (the first hackathon to ever take place in Haiti), H4D2, and #EveryoneHacks. Brugh is a co-founder of Jigsaw Renaissance, a learning and making community in Seattle; co-founder and past director of Space Federation, linking together hacker and maker spaces; current director Geeks Without Bounds; and Fellow at the Berkman Center for Internet & Society.

Monica Bulger is a Fellow at the Berkman Center for Internet & Society and an educational researcher contributing policy research to multi-national groups such as UNICEF, ECPAT, and the European Commission. Her work focuses on the implications of technology use for youth with a particular focus on learning, safety, and empowerment. In this challenging, fast-changing research environment, she aims to identify cognitive, developmental, and attitudinal trends that transcend popular technologies

and speak to deeper purposes for everyday practice.

Neal Cohen is a New York and English qualified lawyer in the Privacy & Security practice group at Perkins Coie LLP, where he assists multinational organizations with their European and global data protection and privacy law compliance strategies. This frequently includes advising on privacy and security policies, terms and conditions for use, data security breaches, interactions with governmental authorities, the cross-border transfer of personal data, cloud computing, big data, mobile applications and data privacy lobbying strategies. As a Fellow at the Berkman Center for Internet & Society, he researches and analyzes the global convergence of data protection and privacy laws and their greater impact on society.

Tim Davies works on projects at the intersection of civic engagement, technology, facilitation and community engagement. He is currently working with the Web Foundation as coordinator of the research and capacity building Exploring the Emerging Impacts of Open Data in Development Countries project, and through Practical Participation on the development of data standards for transparency in philanthropy. He is an Affiliate at the Berkman Center for Internet & Society.

Adrienne Debigare is a product manager at Boston.com, a research affiliate at the MIT Center for Civic Media, and a research assistant at the Berkman Center for Internet & Society. She is interested in the effects of technology on civic engagement and steering the adoption of new technology within journalism to promote the ethical use of data.

Primavera De Filippi is a postdoctoral researcher at the CERSA / CNRS / Université Paris II (Panthéon-Assas). She is currently a Fellow at the Berkman Center for Internet & Society at Harvard Law School, where she is investigating the legal challenges of "governance-by-design" in online distributed architectures, such as Bitcoin and Ethereum.

Andy Ellis is Akamai's Chief Security Officer, responsible for overseeing the security architecture and compliance of the company's massive, globally distributed network. He is the designer and patentholder of Akamai's SSL acceleration network, as well as several of the critical technologies underpinning the company's Kona Security Solutions. Ellis is an Affiliate at the Berkman Center for Internet & Society.

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.

Sands Fish is a data scientist and computational artist. He is a Fellow at the Berkman Center for Internet & Society and a Research Affiliate at MIT's Center for Civic Media. He is also a Digital Humanities Fellow at MIT's HyperStudio and organizes the Boston Creative Coders collective. He focuses on information aesthetics, network analysis, and text mining, applying these to reveal and map patterns in networked data structures such as the social web and linked open data.

Nathan Freitas leads the Guardian Project, an open-source mobile security software project, and directs technology strategy and training at the Tibet Action Institute. He is a Fellow at the Berkman

Center for Internet & Society, where his work focuses on tracking the legality and prosecution risks for mobile security apps users worldwide.

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). 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.

Rebekah Heacock Jones is a Senior Project Manager at the Berkman Center for Internet & Society. Since joining the Center in 2009, she has managed the OpenNet Initiative, Digital Public Library for America, and Internet Monitor projects, among others; she also leads the Internet Health practice group. She previously co-directed the Global Voices Technology for Transparency Network.

Alison Head is a Research Scientist in the Information School at the University of Washington, a Faculty Associate at the Berkman Center for Internet & Society, and the Executive Director of Project Information Literacy (PIL), a public benefit nonprofit dedicated to conducting ongoing, large-scale research about college students and their research habits and strategies in the digital age. Since 2008, PIL has studied over 11,000 students on 60 US campuses. PIL has investigated how college students conduct research and find information for their coursework and for dealing with the demands of their everyday lives.

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.

Ethan Katsh is Professor Emeritus of Legal Studies at the University of Massachusetts Amherst, Director of the National Center for Technology and Dispute Resolution, and an Affiliate at the Berkman Center for Internet & Society. He is recognized as a founder of the field of online dispute resolution (ODR) and has served as principal dispute resolution consultant for the Office of Government Information Services (OGIS), a federal agency mandated to provide mediation in Freedom of Information Act disputes. He is currently assisting the National Opinion Research Center (NORC) in a study of disputes involving electronic medical records.

Vivek Krishnamurthy is a Clinical Instructor in Harvard Law School's Cyberlaw Clinic, based at the Berkman Center for Internet & Society. He specializes in the international aspects of Internet governance and on the human rights challenges associated with offering new Internet-based services in different legal environments around the world. Krishnamurthy is a graduate of the University of Toronto, Yale Law School, and the University of Oxford, where he was a Rhodes Scholar. Prior to

joining the Cyberlaw Clinic, he clerked for the Hon. Morris J. Fish of the Supreme Court of Canada and worked as an associate in the International and Corporate Social Responsibility Practices at Foley Hoag LLP.

James Losey is a PhD candidate with the School of International Studies and the Department of Media Studies at Stockholm University in Sweden working on a dissertation focused on the tensions between states and Internet companies and the relationship to national sovereignty, citizenship, and the flow of information. He is an Affiliate at the Berkman Center for Internet & Society and a visiting scholar at the University of Pennsylvania's Center for Global Communication Studies at the Annenberg School for Communication. Previously, he has been a Google Policy Fellow with the Global Network Initiative and a Consortium on Media Policy Studies fellow.

Alessandro Mantelero is aggregate professor of Private Law at the Polytechnic University of Turin and Director of Privacy and Faculty Fellow at the Nexa Center for Internet and Society. His research is focused on data protection, big data, and privacy. Mantelero was a Visiting Researcher at the Berkman Center for Internet & Society in 2012.

Helmi Noman is a Research Affiliate at the Berkman Center for Internet & Society. His research focuses on the Internet, media and telecommunications laws, and issues surrounding filtering and censorship in the Middle East and North Africa region. He also explores the impact of information and communication technologies on the Arab information societies, Arabic web content, how the use of the Internet defies the social and political structures in the region, and the potential systemic changes cyberspace can bring to real space in the Arab region.

David R. O'Brien joined the Berkman Center for Internet & Society staff as a project coordinator in February 2011. He has been contributing legal and policy research to a number of Berkman Center 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.

Dalia Othman is a Fellow at the Berkman Center for Internet & Society and a Visiting Scholar at MIT's Center for Civic Media. At the Berkman Center, she looks at online civic engagement in the Arab World, focusing on analyzing the Arab Blogosphere and Twitter maps of various countries within the region. She dedicates the rest of her time to exploring different themes around digital storytelling and is currently building a resource platform that will help communities tell powerful stories online.

Jiou Park is a research assistant at the Berkman Center for Internet & Society and a first year Masters in Theological Studies student at Harvard Divinity School with a focus on Religion and Social Sciences. She has worked as a human rights and civil rights advocate, especially in areas of national security and racial justice. Her experience in rights advocacy has taught her the crucial role new technologies can play in empowering or dispossessing communities, and in constructing identities, leading to an interest in the intersection of technology, religion, culture, and policy.

Jonathon W. Penney is a lawyer, a Research Fellow at the Citizen Lab / Canada Centre for Global Security Studies, Munk School of Global Affairs, University of Toronto, an Affiliate at the Berkman Center for Internet & Society, and a doctoral student in information communication sciences at the

Oxford Internet Institute, University of Oxford, where his interdisciplinary research explores regulatory chilling effects online.

Shawn Powers is an assistant professor in the Department of Communication at Georgia State University. His research specializes in international political communication with particular attention to the geopolitics of information and technology policy. He is a faculty affiliate of GSU's Transcultural Violence and Conflict initiative and co-leads its British Council and US Institute of Peace-funded project on Civic Approaches to Religious Conflict. He is also an associate director at the Center for International Media Education and serves on the Board of Advisors for the US Advisory Commission on Public Diplomacy.

Orna Rabinovich-Einy is a Senior Lecturer at the Faculty of Law at the University of Haifa and a Fellow at the National Center for Technology and Dispute Resolution. Her areas of expertise are alternative dispute resolution (ADR), online dispute resolution (ODR), and civil procedure, with research focusing on the relationship between formal and informal justice systems, dispute resolution system design and the impact of technology on dispute resolution.

Jordi Rodriguez Virgili is Assistant Dean and Professor of the School of Communication at the University of Navarra, where he teaches Political Communication, Electoral Campaigns, and Contemporary Political Systems. He is a Researcher at The Center for Internet Studies and Digital Life, affiliated with the School of Communication at the University of Navarra and the Director of the Master's program in Political and Corporate Communication. He is involved in qualitative and quantitative research projects on the impact of ICTs in politics and election campaigns. He was previously a visiting professor at the Graduate School of Political Management (GSPM) at the George Washington University.

Charo Sádaba is Assistant Dean for Research and Postgraduate Programs of the School of Communication at the University of Navarra, where she is also on the Board of Directors of the Center for Internet Studies and Digital Life. She teaches Interactive Marketing to undergraduate and graduate students. Her research is focused on how technological innovations affect media companies' business models. Since 2001 she has also been involved in several qualitative and quantitative research projects on the impact of ICTs on youth with an international scope. She is also independent expert for the EU Safer Internet Programme.

Sophia Sadinsky is the Princeton in Latin America Fellow at the Center for Studies on Freedom of Expression and Access to Information (CELE) at the Universidad de Palermo.

Andy Sellars is the Berkman Center for Internet & Society's Corydon B. Dunham First Amendment Fellow, and works at the Harvard Law School Cyberlaw Clinic. He previously was the Assistant Director of the Berkman Center's Digital Media Law Project. He studies Internet free speech and intellectual property matters.

David Sangokoya recently graduated with a MPA degree from NYU Wagner. Prior to Wagner, he has worked with nonprofits in northern Uganda, Liberia, Namibia, and Sri Lanka. Building off his research and project experiences in post-conflict environments, he is interested in how data and technology can help governments protect the rights of the disadvantaged, make better allocation decisions, and

create much needed mechanisms for good governance strategies.

Hasit Shah is a senior producer at BBC News in London and was a 2014 Nieman-Berkman Fellow in Journalism Innovation at Harvard. He is an Affiliate at the Berkman Center for Internet & Society. He has been researching the impact of the rapidly rising numbers of Internet users in India—driven by increasingly inexpensive smartphones—on digital news platforms and business models.

Stefaan G. Verhulst is Co-Founder and Chief Research and Development Officer of the Governance Laboratory @NYU (GovLab), where he is responsible for building a research foundation on how to transform governance using advances in science and technology. Verhulst's latest scholarship centers on how technology can improve people's lives and the creation of more effective and collaborative forms of governance. Specifically, he is interested in the perils and promise of collaborative technologies and how to harness the unprecedented volume of information to advance the public good.

Clarence Wardell III is a researcher and social entrepreneur who is passionate about using technology to increase and enhance civic engagement. He is currently a Fellow at the Berkman Center for Internet & Society. Previously, he was a Research Scientist with CNA Corporation's Safety & Security group, where he provided analytical support to emergency management and law enforcement organizations to improve response outcomes. In that role, he also led CNA's research on the adoption and use of new media technologies by emergency managers and law enforcement agencies.

Sara M. Watson is a technology critic and a Fellow at the Berkman Center for Internet & Society. Her work addresses how individuals are learning to live with, understand, and interpret data. She is interested in the interactions between users, data and algorithms, and the internet platforms that mediate and govern digital experiences. Her writing has appeared in The Atlantic, Al Jazeera America, Wired, Harvard Business Review, and Slate.

Rolf H. Weber is Chair Professor for Civil, Commercial and European Law at the University of Zurich, Switzerland, Visiting Professor at the University of Hong Kong, and Attorney-at-Law in Zurich. His contribution is partly based on his book Realizing a New Global Cyberspace Framework, Normative Foundations and Guiding Principles, Zürich 2014.

Jonathan Zittrain is the George Bemis 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, Vice Dean for Library and Information Resources at the Harvard Law School Library, 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.