INTERNET FREEDOM AND THE ROLE OF AN INFORMED CITIZENRY AT THE DAWN OF THE INFORMATION AGE

Sascha Meinrath[*]
Marvin Ammori[**]

More than sixty years ago, civil rights activists realized that the most effective route to bettering our country was through mass social movements, civil disobedience, and judicial review. Those whom we hold up today as champions from this era—from Rosa Parks and Thurgood Marshall to Malcolm X and Martin Luther King, Jr.—were part of sophisticated, nationwide, legal interventions to stand up for what they believed. To be an informed citizen and an active member of civil society during this epoch was to be aware of these battles and even participate in them—taking sides on the street, at the lunch counters, in the pages of the nation's newspapers, and through broadcast radio and television. In law school, reading *Brown v. Board of Education*[1] and *Cooper v. Aaron*,[2] you might get the mistaken impression that the judicial branch was the focus of the debate, or the most important agent of change. But this litigation was a purposeful and well-thought-out facet of a far broader social movement and organizing strategy.[3] This social movement focused on a key normative question for civil society: Who can participate in our democracy as a full citizen—with an equal vote, equal treatment under the law, equal access to education, and all the other social resources necessary to enjoy true liberty—and have a meaningful say in our government?[4]

Today we are at a similar critical juncture, asking similar questions about participation in modern civil society.[5] We have made progress in making our

---

[*] Vice president of the New America Foundation and director of the Open Technology Institute.

[**] Bernard L. Schwartz Fellow, New America Foundation and Principal of the Ammori Group law firm. Harvard, J.D., Michigan, B.A.

[1] Brown v. Bd. of Educ., 347 U.S. 483 (1954).

[2] Cooper v. Aaron, 358 U.S. 1 (1958).

[3] *See* Stephen C. Yeazell, Brown, *The Civil Rights Movement, and the Silent Litigation Revolution*, 57 VAND. L. REV. 1975, 1975–81 (2004).

[4] *See* James Thomas Tucker, *Affirmative Action and [Mis]representation: Part 1 – Reclaiming the Civil Rights Vision of the Right To Vote*, 43 HOW. L.J. 343, 367–72 (2000).

[5] *See* PAUL STARR, THE CREATION OF THE MEDIA: POLITICAL ORIGINS OF MODERN COMMUNICATIONS 19 (2004).

democracy more racially inclusive, although controversies remain over de facto segregation and voter discrimination.[6] But while the foundation of our democracy includes the right to vote, it also requires the right to access information and disseminate information to others.[7] The Constitution terms it the right to freedom of speech and press, while the Universal Declaration of Human Rights calls it the right to opinion and expression.[8] Today the most powerful tools to amplify our thoughts and ideas are often not newspapers and broadcast stations, controlled by the few and the powerful.

The most powerful tool for a large and growing global constituency is an open Internet and the applications we use every day—from Facebook and Twitter to YouTube and Tumblr. The Internet has become the core infrastructure of modern free expression and speech. By connecting us, the free and open Internet is the foundation for twenty-first century civil society. The enemies of a robust, democratic civil society know this. It is why Internet freedom is under sustained attack.

The battle over Internet freedom will have a profound impact on the future of civil society and democracy. These attacks sometimes take the form of legislation in cybersecurity or copyright. For example, Senator Lieberman pushed to introduce legislation granting the President authority to shut down the Internet by creating a central "kill switch"—legislation that was only buried when Egypt's President Mubarak used a similar system to take that country offline during its own democratic protests.[9] Congress also nearly passed the hugely controversial Stop Online Piracy Act[10] ("SOPA"), which is often derisively called the Stop Online *Privacy* Act, and Protect Intellectual Property Act[11] ("PIPA")—bills that resulted in a Wikipedia blackout on January 18, 2012.[12]

---

[6] Editorial, *In Defense of Voting Rights*, N.Y. TIMES, May 20, 2012, at SR10; Dan Rivoli, *AG Holder Defends Embattled Voting Rights Act*, INT'L BUS. TIMES (May 23, 2012), http://www.ibtimes.com/ag-holder-defends-embattled-voting-rights-act-699735.

[7] *See* JOHN HART ELY, DEMOCRACY AND DISTRUST: A THEORY OF JUDICIAL REVIEW 112, 116 (1980).

[8] U.S. CONST. amend. I; Universal Declaration of Human Rights, G.A. Res. 217 (III) A, art. 19, U.N. Doc. A/RES/217 (Dec. 10, 1948).

[9] Nick Eaton, *Internet 'Kill Switch' Is Dead, But Bill Calls for Cybersecurity Plan*, SEATTLEPI.COM (Feb. 19, 2011), http://www.seattlepi.com/national/article/Internet-kill-switch-is-dead-but-bill-calls-1022941.php.

[10] Stop Online Piracy Act, H.R. 3261, 112th Cong. (2011).

[11] Protect Intellectual Property Act, S. 968, 112th Cong. (2011).

[12] Sarah Maslin Nir, *Wikipedia Blackout Lets in Some Light*, N.Y. TIMES BITS BLOG (Jan. 18, 2012, 1:38 AM), http://bits.blogs.nytimes.com/2012/01/18/wikipedia-blackout-lets-in-some-light.

Decisions being made right now in Washington, D.C., will affect the very trajectory of democracy. Too often, proposed decisions are at odds not only with freedom, but also with technological reality. D.C. is, first and foremost, a city of lawyers. Unfortunately, these lawyers think themselves to be technologists and are running rampant, drafting remarkably bad laws—usually not through malfeasance, but through ignorance. Thus, there is a crucial opportunity to change the course of history simply by ensuring that key decision-makers actually understand technology, its limits, and what it makes possible. To analogize to an earlier era, the decision in *Brown v. Board of Education* turned on psychological evidence concerning children in segregated schools.[13] Imagine if lawyers based their case on their "gut feeling" rather than relying on social psychological experts and research based upon empirical data.

Sascha directs the Open Technology Institute at the New America Foundation ("OTI").[14] The New America Foundation is a public interest think tank in Washington, D.C., whose programs span everything from foreign policy analysis to educational reform, and from asset building amongst the poor to how to remake our medical system to be both more affordable and more responsive. The Open Technology Institute is the technology and telecom arm of the New America Foundation's work—a group of technologists working to counter the misinformation campaigns currently running rampant in D.C.

Marvin is one of the few lawyers welcomed to hang out at the Open Technology Institute. He is a veteran of the open Internet battles and the SOPA battle, a First Amendment scholar, and once served as the head lawyer of Free Press. Most importantly, he tries to wield technical know-how to bolster his legal acumen.

Simply put, to defend Internet freedom at this critical juncture, we need not only legal expertise but also *technological* expertise. Interested parties—both corporations and entrenched bureaucracies—take advantage of the woeful technological naiveté of most politicians, regulators, and key administration officials. Sowing "Fear, Uncertainty, and Doubt" ("FUD") is often their modus operandi. And this FUD has, for far too long, driven a national debate over

---

[13] Brown v. Bd. of Educ., 347 U.S. 483, 494 (1954) ("To separate [children] from others of similar age and qualifications solely because of their race generates a feeling of inferiority as to their status in the community that may affect their hearts and minds in a way unlikely ever to be undone.").

[14] OPEN TECH. INST., http://www.oti.newamerica.net (last visited Sept. 23, 2012).

cybersecurity, copyright, surveillance, and open Internet policies. This FUD is directly undermining our ability, as a democratic society, to protect human rights online.

Much of the work that OTI does focuses on educating key decision makers—at the Federal Communications Commission, Federal Trade Commission, State Department, and White House; in the Senate and House of Representatives; and at leading advocacy organizations—about technological reality. But the forces of FUD are powerful, and OTI has a modest team of some fifty tech-savvy staff. What is needed today is a far more widespread intervention—with help from technologists across the country and from average Americans, who often know far more about technology than the average policymaker in D.C.

But why would you want to help? For the same reason you would want to take part in the great debates over civil rights and civil society in the 1950s and 1960s. What stories do we want to be able to tell our children and our grandchildren? We have a once-in-a-lifetime, perhaps a once-in-a-century, opportunity. As we transition into the Information Age, we must ask ourselves: How do we support a twenty-first century *civil society* that is inclusive, decentralized, and free—the kind of society where participatory democracy thrives?

Our short Article discusses three examples of legal debates that will shape the future of democracy. The first focuses on the U.S. State Department and international Internet freedom. The second focuses on SOPA and PIPA as exemplars of extreme copyright laws that directly undermine Internet freedom and free speech. The third focuses on the mesh networking technologies we are creating at OTI with grants from the State Department to circumvent surveillance and censorship. For each we have a choice, or many choices, that will determine who can speak to whom, how, and with whose permission.

I. THE HILLARY CLINTON DOCTRINE AND THE ARAB SPRING

"Internet freedom" is a purposefully nebulous concept. It encompasses notions of social and economic justice, the right to communicate and disseminate information, and the opportunity to use online resources without fearing discrimination or retribution.

While long discussed amongst hackers and human rights workers, Internet freedom has only recently entered the realm of statecraft and international

diplomacy. And this recent ascendancy is very much due to the efforts of a single individual: U.S. Secretary of State Hillary Rodham Clinton.

On January 21, 2010, Clinton threw down the gauntlet, shifting America's foreign policy to address virtual communications and signaling to governments around the globe that the online world, much like the offline world, was within the purview of the most powerful democratic force in the entirety of human history.[15] And at the crux of this new twenty-first century statecraft was the realization that connectivity, like any powerful tool, was a Faustian bargain. As Secretary Clinton summarized:

> [A]mid this unprecedented surge in connectivity, we must also recognize that these technologies are not an unmitigated blessing. These tools are also being exploited to undermine human progress and political rights. . . . The same networks that help organize movements for freedom also enable al-Qaida [sic] to spew hatred and incite violence against the innocent. And technologies with the potential to open up access to government and promote transparency can also be hijacked by governments to crush dissent and deny human rights.[16]

Sascha spoke with Clinton's staff prior to the event, and it was clear then that a new trajectory was about to be mapped out. But even while listening to her powerful speech at the event, Sascha couldn't help but wonder how a single entity—no matter how powerful—could possibly achieve the kind of global intervention that was envisioned.

In fact, it seemed the height of hubris for the United States, as creators and purveyors of some of the most advanced online surveillance and monitoring technologies on the planet, to be the champion of Internet freedom.

While the goals laid out by Secretary Clinton were laudable, there needed to be some sort of catalyst to move the discussion beyond inside-the-beltway rhetoric and unilateral interventions. To raise the priority level of Internet freedom, galvanize an international, multilateral response, and heighten awareness of its importance to the global community, we needed a catalyst—a Boston Tea Party on a much larger scale.

---

[15] Hillary Rodham Clinton, U.S. Sec'y of State, Remarks on Internet Freedom at the Newseum (Jan. 21, 2010), *available at* http://www.state.gov/secretary/rm/2010/01/135519.htm.

[16] *Id.*

On December 17, 2010, less than a year after Clinton's Internet freedom speech, Mohamed Bouazizi's self-immolation sparked a series of cascading protests against oppression that spread and became known as Arab Spring.[17]

Over the ensuing months, the toppling of governments by revolutionary movements in Tunisia, Egypt, and Libya,[18] along with widespread civil disobedience and government concessions throughout the Middle East and Northern Africa, as well as ongoing battles in Syria and Yemen (where their ruler, Ali Abdullah Saleh, stepped down at the end of February)[19] demonstrated both the enormous impact of Bouazizi's actions as well as the power of online communications as a tool for pro-democracy organizing.

We do not like using phrases like "Twitter Revolution" and "WikiLeaks Revolution" because these technologies are merely useful tools—they are accelerants or sparks—but not the underpinnings or foundations for the protests they are a part of. In much the same way, pamphlets did not create the American Revolution, but pamphleteers were certainly a part of the galvanization of protests against King George III.[20] But we are not among those who think that Internet played no role. Marvin attended an event at a very influential foreign policy think tank on the one-year anniversary of the beginning of the Arab Spring. The event featured four Middle East policy experts discussing the Arab Spring. After an hour of discussion of food prices and the family habits of the country's leaders, the moderator threw open the discussion to audience questions. The first question was from a man who looked like he was eighty years old, but even he wondered, "Why didn't you experts ever once mention the role of social media or the Internet in your entire discussion about the Arab Spring?" And the experts, true to form, said they didn't mention social media and the Internet because it wasn't important for the Arab Spring. This assessment is clearly wrong, as basic common sense would reveal. However, the foreign policy community has its share of Luddites who are as out of touch with the technologies most of us use every day as the

---

[17] Rania Abouzeid, *Bouazizi: The Man Who Set Himself and Tunisia on Fire*, TIME (Jan. 21, 2011), http://www.time.com/time/magazine/article/0,9171,2044723,00.html.

[18] *See* Shashank Joshi, *Film Protests: What Explains the Anger?*, BBC NEWS (Sept. 15, 2012), http://www.bbc.co.uk/news/world-middle-east-19609951.

[19] Brian Whitaker, *Yemen's Ali Abdullah Saleh Resigns–But It Changes Little*, GUARDIAN (Nov. 24, 2011), http://www.guardian.co.uk/commentisfree/2011/nov/24/yemen-ali-abdullah-saleh-resigns.

[20] Homer L. Calkin, *Pamphlets and Public Opinion During the American Revolution*, 64 PA. MAG. HIST. & BIOGRAPHY 22, 22–23 (1940).

technodeterminists who view Arab Spring as resulting from the existence of Twitter and Facebook.

For Internet freedom advocates, the Arab Spring was itself a singularly powerful catalyst—catapulting the ideas behind twenty-first century statecraft to the forefront of international diplomacy efforts. Until then—and even afterwards for some—foreign policy experts would ignore the importance of connection tools, suggest nothing had changed, and focus on the "history" and "culture" that these experts had studied and written about, not the technologies they too often did not understand.

All of a sudden, issues of online censorship and the lengths some authoritarian regimes would go to prevent the free flow of information (as exemplified by Egypt's President Hosni Mubarak completely disconnecting Egypt from the Internet),[21] were paramount. Connectivity was paramount. Our human rights and freedom of expression online became paramount.

The very transnational nature of most social media—much like the distributed nature of printing presses in prior eras—has made it extremely difficult for authoritarian regimes (or any government, as we will see) to eliminate online content or prevent the dissemination of information.

As one can see from Secretary Clinton's December 8, 2011, rhetoric, the solutions to many of these problems require a multilateral, transnational, framework. Internet freedom needed its own "coalition of the willing"—countries like Sweden, France, the Netherland, Brazil, and Australia needed to unite. As Secretary Clinton stated:

> Delivering on internet freedom requires cooperative actions, and we have to foster a global conversation based on shared principles . . . . It requires an ongoing effort to reckon with the new reality that we live in, in a digital world, and doing so in a way that maximizes its promise.[22]

Until the Arab Spring, international diplomacy around online issues had focused almost entirely on copyright and law enforcement. But following that catalyst, human rights became the organizing lens. Internet freedom prioritized

---

[21] James Glanz & John Markoff, *Egypt's Autocracy Found Internet 'Off' Switch for Internet*, N.Y. TIMES, Feb. 15, 2011, at A1.

[22] Hillary Rodham Clinton, U.S. Sec'y of State, Remarks at the Conference on Internet Freedom (Dec. 8, 2011), *available at* http://www.state.gov/secretary/rm/2011/12/178511.htm.

a focus on surveillance and monitoring, not as tools for good, but as problems to be circumvented.

The Arab Spring catapulted a new group of visionaries to the forefront of the State Department's policymaking: the "Internet Freedom Fighters."

But because governments and other big bureaucracies (especially media conglomerates and law enforcement agencies) tend to pivot slowly, there are still a tremendous number of people mired in more of a "command and control" mentality predicated upon total information awareness and the lock-down of networking technologies that could be used for ill. These people we call the "Cold Warriors."

And here we come to the first crux of the behind-the-scenes battles that are happening in Washington, D.C., today. These fights often happen outside of public view, but their outcomes will reverberate around the globe and across generations. These fights were caused by decades of diplomacy that expected human rights to arise from economic and governmental stability, and too often failed to evolve and take account of a post-Cold War, computer-mediated world.

Current policy debates are divorced from technological reality in several ways, the most important of which is the assumption that we can encourage Internet freedom and privacy abroad, but condone Internet control and mass surveillance at home. We condemn countries that block websites because of political speech or because they violate social norms (e.g., pornography).[23] Yet a coalition of Hollywood studios and the Congressmen whom they fund argued that we should block websites based on copyright concerns.[24] Cable and phone companies—and the Congressmen they fund—argue for the right to block and discriminate against websites and technologies to maximize their profits.[25] At the same time, we condemn the widespread use of surveillance abroad. We condemn other countries for using surveillance technologies created by

---

[23] David Morgan, *Obama Decries Iran's "Electronic Curtain,"* CBS NEWS (Mar. 20, 2012), http://www.cbsnews.com/8301-250_162-57400698/obama-decries-irans-electronic-curtain.

[24] Declan McCullagh, *SOPA Attracts Plenty of Supporters During House Debate*, CNET NEWS (Dec. 15, 2011), http://news.cnet.com/8301-31921_3-57344021-281/sopa-attracts-plenty-of-supporters-during-house-debate.

[25] Jason Mick, *U.S. House Votes To Allow Cable Providers To Throttle Internet*, DAILYTECH (Feb. 18, 2011, 11:04 AM), http://www.dailytech.com/US+House+Votes+to+Allow+Cable+Providers+to+Throttle+Internet/article20947.htm.

companies like Blue Coat.[26] We condemn other countries that push for technological backdoors in Internet technologies, backdoors that would permit those countries to surveil their citizens.[27] But companies like Blue Coat are Western businesses, creating technologies to be used all over the world.[28] Our nation's own law enforcement and intelligence agencies want backdoors built into online technologies so they can spy on foreign citizens and local residents alike, even if the exploits place Americans at greater risk of identity theft and spying, even if the exploits place Chinese dissidents and Syrian dissidents at risk.[29] When we place backdoors into Skype and Facebook, it is not just the NSA and the FBI who have access. We also have overbroad legal policies that permit surveillance at home, though some companies have begun fighting against these excesses—Twitter, for example, has stood up and fought secret subpoenas for the direct messages of organizers of the Occupy Movement.[30] We have to make a decision: whether we choose an Internet whose basic technologies and laws supports security *and* Internet freedom, or an Internet that does not.

II. PIRACY IS THE PRICE WE PAY FOR CIVILIZATION

Sascha's daughter, Clara, is now two years old—she will never know a world without connectivity. She will pick up his phone (or anything with buttons on it—a TV remote, computer mouse, or Wii controller), hold it to her ear, and say, "Hello?"

She knows that devices connect her to other people—she has learned that when she Skypes with her father, he is not actually on the other side of the laptop screen, but somewhere else entirely.

---

[26] Blue Coat and companies like it "are selling technologies that enable the repressive Iranian and Syrian regimes to disrupt and monitor the Internet and track down government critics . . . ." Editorial, *Unplug Companies That Help Iran and Syria Spy on Citizens*, BLOOMBERG (Apr. 24, 2012), http://www.bloomberg.com/news/2012-04-24/unplug-companies-that-help-iran-and-syria-spy-on-citizens.html.

[27] Deborah Charles, *U.S. Says UAE BlackBerry Ban Sets Dangerous Precedent*, REUTERS, Aug. 2, 2010, *available at* http://www.reuters.com/article/2010/08/02/us-uae-blackberry-usa-idUSTRE67144P20100802.

[28] Richard Levick, *Surveillance Technology Firms Face Reputational Bust amid Business Boom*, FORBES (Jan. 18, 2012), http://www.forbes.com/sites/richardlevick/2012/01/18/surveillance-technology-firms-face-reputational-bust-amid-business-boom/2.

[29] Kim Zetter, *FBI Wants Backdoors in Facebook, Skype and Instant Messaging*, WIRED (May 4, 2012), http://www.wired.com/threatlevel/2012/05/fbi-seeks-internet-backdoors.

[30] Andy Greenberg, *Twitter Fights Prosecutors Seeking Occupy Protester's Data Without Warrant*, FORBES (May 8, 2012), http://www.forbes.com/sites/andygreenberg/2012/05/08/twitter-fights-prosecutors-seeking-occupy-protesters-data-without-warrant.

Her notion of the world will not be divided into "online" and "offline," like ours is today; she will expect seamless integration. In her world, offline and online rights are not dichotomous—they are just rights, and she will expect them to be universal.

All of this means that we still have a long way to go to ensure that our rights in a free society do not end when you log onto the Internet. Today, there is an open question of whether we should enjoy the same rights online as we do in the rest of our lives.

At this moment in history, the Internet Freedom Fighters are ascendant, but media conglomerates are fighting for ever more powerful surveillance mechanisms to enforce copyright. And, by aligning themselves with law enforcement, these companies have created an incredibly powerful lobby—a lobby that seeks to all but eliminate meaningful anonymity and privacy online.

This battle is epitomized by legislation introduced in Congress in 2012—SOPA and PIPA. These two bills were borne of an unbelievable ignorance of both technological reality and the egregiously bad ramifications that these laws would have.

Unfortunately, many Congressional staffers who initially supported these bills had no idea what the bills actually did. What these staffers did know was that the Recording Industry Association of America ("RIAA") and Motion Picture Association of America ("MPAA")—together, the largest and most powerful copyright lobby in the world—wanted these laws passed.[31] So did the Chamber of Commerce and the American Federation of Labor and Congress of Industrial Organizations.[32] Why did they need to understand the technological implications of a proposed law when they knew the supporters included such powerful organizations?

Apparently, for the RIAA and MPAA, the notion of protecting the fundamentals of a free society is secondary to the elimination of media piracy. Studios and labels have a fiduciary duty to their shareholders to maximize profit, and if the open Internet is the collateral damage, so be it. This copyright *über alles* mentality is one of the key problems we now face as we attempt to transition to a human rights framework for international statecraft.

---

[31] Ian Chant, *MPAA, RIAA Would Like Some Help from the Government in Fighting Piracy, Please*, GEEKOSYSTEM (Aug. 13, 2012, 1:45 PM), http://www.geekosystem.com/mpaa-riaa-government-piracy.

[32] Mike Masnick, *Would Obama Veto SOPA? Extremely Doubtful*, TECHDIRT (Dec. 27, 2011, 1:20 PM), http://www.techdirt.com/articles/20111226/23082117192/would-obama-veto-sopa-extremely-doubtful.

If one reads the Constitution's Copyright Clause, and not the Supreme Court's apparent interpretation of it, copyright is a means to an end. The Constitution empowers Congress:

> *To promote the Progress of Science and useful Arts*, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries . . . .[33]

We believe the purpose of copyright is to ensure that science and the useful arts continued to progress. To accomplish this, Congress originally set copyright for a term of fourteen years.[34] To put this into perspective, as of this writing, this would have put everything from 1999 on back (from movies, to music, to books, to video games) into the public domain. Yet today, nothing copyrighted since 1923 has entered the public domain. So what happened?

For decades, copyright interests have systematically extended copyright (de facto, forever). Every time copyright was to run out, a law was passed to extend it. Today, copyright extends for the entire life of the author plus seventy years; corporations get a flat ninety-five years.[35] So if 1923 + 95 years brings us to 2018, we should expect another attempt for a "limited time" extension to copyright before then.

But copyright was always, first and foremost, meant "to promote the progress of Science and useful Arts,"[36] which were perceived to be the underpinning of an enlightened society. We would argue that some piracy is the price we pay to live in a free society—just as some real-world crime is also expected. But, of course, you cannot say this in Washington, D.C.—you cannot say, "I'd rather live in a society with piracy than in one intent on rooting it out by any means necessary."

The Internet has always been, from its genesis, a tool for swapping information amongst participants. And as the power of this tool has grown exponentially, far beyond what anyone could have possibly imagined, so too has our responsibility to act as defenders and champions of its openness and fundamentally participatory nature.

Even more importantly, we have a responsibility to teach future generations to improve upon what we have created and ensure that the Internet's next

---

33 U.S. CONST. art. I, § 8, cl. 8 (emphasis added).
34 Act of May 31, 1790, ch. 15, § 1, 1 Stat. 124 (1790) (repealed 1831).
35 17 U.S.C. § 302 (2006).
36 U.S. CONST. art. I, § 8, cl. 8.

iterations are more inclusive, less discriminatory, and increasingly supportive of our fundamental, inalienable human rights.

The best way we can do this is to ensure that our pedagogical practices not only empower students with the digital literacy skills they need to navigate online resources, but also that they have the critical thinking and organizing skills necessary to actively defend themselves against online threats of censorship, surveillance, and discrimination.

After the Arab Spring, the world's dictators are getting better at fighting for control. Oppressive elements are engaging in more and more insidious efforts to surveil, monitor, and censor communications. Our sometimes laissez-faire stance toward the Internet makes us ill-prepared to face today's grim truth: Powers, both foreign and domestic, are seeking unprecedented control over how we communicate.

And while it would be unjust to equate the actions of Iran with those of the RIAA and MPAA, the technologies used by Iran to identify banned content, services, and applications are the same ones used by American authorities and corporations for their own purposes.[37]

Which brings us to another conundrum in the battle between the Internet Freedom Fighters and the Cold Warriors—how do we empower free society while creating technological mechanisms to police malfeasance? The same "good" surveillance technologies are used regularly for such evil purposes, yet have been so impotent in actually stopping piracy in the first place.

Like any powerful tool, technology offers both tremendous boons for adept users and dramatic new pitfalls for an unsuspecting public. But the battles over SOPA and PIPA give us hope.

In an unprecedented show of solidarity, human rights groups and public interest organizations rallied the high-tech community to oppose these two laws. And the results were staggering: On January 18, 2012, exactly two years after the start of Arab Spring, more than 75,000 websites took part in the Internet blackout, opting to blank out their site to protest the overly broad provisions in these laws that would have shut down many of these same

[37] Jamillah Knowles, *The Current State of Internet Access from Inside Iran*, NEXT WEB (March 23, 2012), http://thenextweb.com/me/2012/03/23/the-current-state-of-internet-access-from-inside-iran.

websites.[38] According to estimates, 162 million people saw Wikipedia's blackout page; 2.4 million SOPA/PIPA-related tweets were sent on that day;[39] and Google had 7 million people sign its own anti-SOPA/PIPA petition.[40] In twenty-four hours, Congress was utterly inundated by a massive virtual demonstration against these proposed laws.

The backlash was swift and hyperbolic. In a *New York Times* editorial, Cary Sherman, CEO of the RIAA, blasted opponents of SOPA and PIPA, claiming that policymakers had "a constitutional (and economic) imperative to protect American property from theft."[41]

In the face of a tsunami of e-mails to legislators, the CEO of the RIAA wrote "how many of those e-mails were from the same people who attacked the Web sites of the Department of Justice, the Motion Picture Association of America, my organization and others as retribution for the seizure of Megaupload?"[42] In essence, in RIAA's mind, citizens petitioning Congress are equated with Anonymous and other hackers engaging in acts of civil disobedience.

But the defeat of SOPA and PIPA, contrary to much of the celebration, was not a win so much as a defensive measure that prevented the opponents of a free and open Internet from scoring another victory against the Internet Freedom Fighters. While the RIAA and MPAA may want to label opponents of its self-serving agenda "criminals" and "demagogues," the reality is that most of us just want a return of *balance*.[43]

Copyright has gotten entirely out of control. It is no wonder that a "substantial majority" of Americans—probably almost every single reader—

---

[38] Andrew Couts, *SOPA/PIPA Blackout: By the Numbers*, DIGITAL TRENDS (Jan. 19, 2012), http://www.digitaltrends.com/web/sopa-pipa-blackout-by-the-numbers.

[39] *Id.*

[40] Timothy B. Lee, *SOPA Protest by the Numbers: 162M Pageviews, 7 Million Signatures*, ARS TECHNICA (Jan. 19, 2012, 1:45 PM), http://arstechnica.com/tech-policy/2012/01/sopa-protest-by-the-numbers-162m-pageviews-7-million-signatures.

[41] Cary H. Sherman, Op-Ed., *What Wikipedia Won't Tell You*, N.Y. TIMES, Feb. 8, 2012, at A27.

[42] *Id.*

[43] Nate Anderson, *RIAA (Sort of) Responds to SOPA Critics, Says Copyright "Offers Little Real Protection,"* ARS TECHNICA (Feb. 27, 2012, 7:30 AM), http://arstechnica.com/tech-policy/2012/02/riaa-sort-of-responds-to-critics-says-copyright-offers-little-real-protection ("When the 'Internet side' looks at online copyright and sees two decades of overreach, they will demand that any path forward bend back towards moderation.").

has engaged in piracy.[44] It is the only sane response to an utterly insane mandate. And because of the massive overreach in copyright enforcement, we are heading for one hell of a major battle as the Internet matures.

Let us return to our earlier observation: We need more geeks in government to ensure Internet freedom. We need a government that relies on real technological expertise. Otherwise, bad ideas become enshrined in federal law all too readily. The argument for bills like SOPA and PIPA are that foreign sites are trafficking in copyrighted materials, like movies and shows, and making that material available in the United States. Hollywood lobbyists convinced Congressmen that one way to stop those sites was to force Internet Service Providers in the United States to cease providing domain name queries to those sites.[45] When you punch the letters "ThePirateBay.org" into your browser's navigation bar, you are entering a domain name. But that domain name is not the same thing as the address that the Pirate Bay's servers use to communicate with other computers. That address is an IP address, a string of four numbers, with each number being a value between 0 and 255 (the 256 values correspond to the 2^8 combinations of an eight-bit number). We are running out of IPv4 numbers (there are only 2^{32} of them, roughly 4.3 billion) and moving to addresses that have 2^{128} numbers, called IPv6 (which is roughly equal to $3.4x10^{38}$ IPv6 addresses).[46] If you had to remember the IP address of ThePirateBay.org, and Google.com, and Facebook.com, and Twitter.com, that would be a lot of numbers—you would, eventually, need some sort of Internet phone book. To make things simpler, you remember words like "Google" and "com" and "Wikipedia" and "org," and a computer owned by your ISP or an independent company will connect the words to the right address. Thus, the domain name lookup acts like a phone book for the Internet—matching names of websites with their IP addresses.

SOPA and PIPA would force your ISP to stop connecting your words to the right address.

Some engineers looked at the law and thought that provision was silly. For a range of technical reasons, it would lead to the widespread blocking of

---

[44] Paul Resnikoff, *Study: A 'Substantial Majority' of Americans Have No Problem with File-Swapping*, DIGITAL MUSIC NEWS (Oct. 15, 2012), http://www.digitalmusicnews.com/permalink/2012/121015buy.

[45] Greg Sandoval, *Hollywood Formally Brings ISPs into the Anti-Piracy Fight*, CNET NEWS (Apr. 2, 2012), http://news.cnet.com/8301-31001_3-57408208-261.

[46] Dave Williams, *An IPv6 Primer For Humans: The Internet's Next Big Thing*, DAVE I/O (May 24, 2011), http://blog.dave.io/2011/05/ipv6-primer.

entirely legal content. As an example, say there is a pirating site called pirate.tumblr.com and the ISP blocks tumblr.com. That is a lot of sites, including Texts from Hillary,[47] whose domain names would no longer work in your browser bar. There have been several examples of such overblocking, including a domain name provider called mooo.com—which blocked roughly ten offending sites and 84,000 completely innocent ones—and several sites affected by a Pennsylvania state law that has similar results.[48] Second, while overblocking innocent sites, domain name blocking does not do a great job of blocking the pirating sites SOPA and PIPA targeted. If you want to get to Pirate Bay, you just look up the IP address and write down that four-number address and use it whenever you are looking for pirated material. Third, and perhaps most importantly, some of the top domain name engineers in the nation raised the alarm that domain name blocking interfered with important cybersecurity initiatives to make the Internet domain system more secure—an initiative centered around a technology known as DNSSEC.[49]

During the congressional markup of the SOPA legislation in the House of Representatives, one Congressman opposed to SOPA, Representative Jason Chaffetz of Utah, stated that we were going to perform an operation on a patient without talking to a doctor.[50] We were going to regulate the Internet without talking to the "nerds."[51] Throughout the rest of the hearing, Congressmen inevitably began their remarks by saying that they were not "nerds," meaning technologists, but also made it clear that they had not even spoken to someone who had expertise in the area about which they were about to pass federal legislation.[52] They should have spoken to technologists earlier, but they seemed more concerned about which lobbyists supported or opposed the legislation, rather than whether the legislation made technological sense.

---

[47] TEXTS FROM HILLARY, http://textsfromhillaryclinton.tumblr.com (last visited Oct. 26, 2012).

[48] Nate Anderson, *Silicon Valley Congresswoman: Web Seizures Trample Due Process (and Break the Law)*, ARS TECHNICA (Mar. 14, 2011, 9:10 AM), http://arstechnica.com/tech-policy/2011/03/ars-interviews-rep-zoe-lofgren. *See generally* Ctr. for Democracy & Tech. v. Pappert, 337 F. Supp. 2d 606, 633–34 (E.D. Pa. 2004) (discussing overblocking caused by DNS filtering).

[49] Steve Crocker et al., *Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the PROTECT IP Bill*, SHINKURO 5, 14, 17 (May 2011), http://www.shinkuro.com/PROTECT%20IP%20Technical%20Whitepaper%20Final.pdf.

[50] Mark Stanley, *SOPA Delay Provides Time To Reflect on Expert Warnings*, CTR. DEMOCRACY & TECH. (Dec. 20, 2011), https://www.cdt.org/blogs/mark-stanley/2012sopa-delay-provides-time-reflect-expert-warnings.

[51] *Id.*; *accord* Cecilia Kang, *Tempers Erupt in House Hearing on Stop Online Piracy Act*, WASH. POST, Dec. 16, 2011, at A27.

[52] David Kravets, *Blacklisting Provisions Remain in Stop Online Piracy Act*, WIRED (Dec. 15, 2011), http://www.wired.com/threatlevel/2011/12/sopa-stalls.

III. POSTAL NETWORKS AND MESH NETWORKS

Historian Richard John wrote a seminal book on the original, All-American, packet-switching network: the United States Post Office.[53] It is a little known fact that at one time, nearly eighty percent of all federal employees worked for the Postal Service.[54] As John's book, *Spreading the News*, relates, the early U.S. Postal Service would deliver a package from anyone to anyone, anywhere in the country, and it would never, ever open your mail.[55] And since eighty percent of the U.S. Government was involved with the post office, it certainly is not hyperbole to state that this function was considered central in forging a national identity.

In much the same way, the Internet lays the foundation for twenty-first century participatory democracy. Sure, people use it for a variety of illegal activities—much like they do with the post office; but that is the price we pay for maintaining and expanding civil society and democracy.

Today, many of the best minds of our generation are busily working on circumvention technologies that support secure and anonymous communications, regardless of the efforts of oppressive regimes to monitor, surveil, and censor these communications. Many of us draw our mandate from Article 19 of the Universal Declaration of Human Rights—a visionary document for 1948—which states:

> Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.[56]

We are motivated, not by a hatred of copyright, but rather, by a love for participatory democracy (and the communications and information dissemination that are its underpinnings). For the Open Technology Institute team, our work has focused on a project to create ad-hoc, mesh wireless communications systems—software that repurposes the hardware that is already widely available (from cell phones to laptops to Wi-Fi routers) into a "device-as-infrastructure" network.

---

[53] RICHARD R. JOHN, SPREADING THE NEWS: THE AMERICAN POSTAL SYSTEM FROM FRANKLIN TO MORSE (1995).

[54] *Id.* at 3 tbl.1.1.

[55] *See id.* at 31.

[56] Universal Declaration of Human Rights, *supra* note 8, art. 19.

Put simply, it would enable you and your friends to create a peer-to-peer communications network using the devices that are already in everyone's pockets. This network would allow people to securely and anonymously communicate both with one another and with the outside world.

The U.S. State Department and the Broadcasting Board of Governors (the entity behind Voice of America, Radio Free Asia, etc.) have funded a multi-million dollar research and development effort to accelerate our work. We call this technology, Commotion Wireless, but when *The New York Times* ran its front page, lead Sunday story on our efforts in summer 2011, they created a meme for our project, the "Internet in a suitcase."[57]

And because of that coverage, we have been contacted by people from just about every country on earth—people who want to use this system in their own backyards. Not just in Iran, Syria, North Korea, and countries with similar oppressive regimes, but across North and South America, Europe, Asia, and Africa.

What is clear is that the pent up demand for communications—especially low-cost or free communications—strikes a chord across humanity. It is, as far as we can tell, a universal desire. While we cannot speak about particular deployments overseas, we can tell you that our test beds in Washington, D.C., Philadelphia, and Detroit (and soon, San Francisco) are already proofing out the systems that will soon be available and implemented far more broadly.

And given the distributed nature of these technologies—there is no central point for surveillance, monitoring, or control—our work brings to the forefront questions about how we want to engage with this new technological reality.

Like any powerful tool, these systems will be used by some participants for malfeasance. Can we be comfortable with that? Or will we choose to live in a society where we outlaw these technologies, regardless of the astoundingly beneficial impact they have on our everyday lives?

In Washington, D.C., claims are still being made that we can create the perfect surveillance and monitoring tools (for copyright and law enforcement), and the perfect circumvention tools (to get around surveillance and monitoring). Much like the paradox of an unstoppable force meeting an immovable object, this debate, as currently formulated, has no resolution.

---

[57] James Glanz & John Markoff, *U.S. Underwrites Internet Detour Around Censors*, N.Y. TIMES, June 12, 2011, at A1.

This is why we need to change how we think about the problems facing us at the dawn of the Information Age and the solutions we devise.

Because our work puts us in direct contact with some of the brightest hackers on the planet, we have already seen near-term technologies that fundamentally alter existing surveillance paradigms and business models. The Serval project in Australia is already meshing together cell phones;[58] Cryptocat allows secure communications through existing (decidedly insecure) social media platforms, such as Facebook chat;[59] post-Megaupload file-sharing systems are being set up as we speak;[60] OpenBTS in California and along with several talented Moscow-based hackers have already developed an open GSM stack, allowing anyone to set up their own cell phone base station.[61]

The questions before us are not whether we should allow these technologies to exist, but rather, whether we want the coming transitions to be graceful or disruptive, and whether we will make policy in these important areas with blissful technological ignorance or the benefit of expertise from the people who understand these transformative technologies.

CONCLUSION

We realize our readers are likely lawyers—and lawyers who will be leaders in our computer-mediated civil society in just a few short years. We urge you to make an effort to understand the Internet's legal and technical underpinnings; your ability to post a story on Tumblr or a picture on Instagram is just the tip of the iceberg. Without understanding what is invisible below the surface, you could formulate untold harms; but likewise, with a modicum of technical acumen to assist your endeavors, you could help the technologically illiterate policymakers in D.C. steer the ship of state clear of impending disaster.

---

[58] Dusan Belic, *Serval Project Improves Disaster Communications, Works Even When There Are No Cell Towers Around*, INTOMOBILE, (Feb. 8, 2011, 12:39 AM), http://www.intomobile.com/2011/02/08/serval-project-disaster-communication.

[59] *The Winners of WSJ's Data Transparency Weekend*, WALL ST. J.: DIGITS BLOG (Apr. 16, 2012, 1:03 PM), http://blogs.wsj.com/digits/2012/04/16/the-winners-of-wsjs-data-transparency-weekend.

[60] Ernesto, *MegaUpload Alternatives See Surge in Traffic After Shutdown*, TORRENTFREAK (Jan. 26, 2012), http://torrentfreak.com/megaupload-alternatives-see-surge-in-traffic-after-shutdown-120126.

[61] Andrew Back, *Building a GSM Network with Open Source*, H OPEN (Mar. 26, 2012, 5:24 PM), http://www.h-online.com/open/features/Building-a-GSM-network-with-open-source-1476745.html.