THE "FREEDOM TO CONNECT" AND INTERNATIONAL INTERNET TRANSPARENCY

ADAM CANDEUB*

The internet and other information technologies have driven much of the political unrest that has shaken the Middle East in recent months. We are only beginning to understand the way these technologies have changed groups' abilities to organize against their governments. Conversely, these technologies have empowered government to better track, monitor, and control their citizenry. On one hand, the Middle East revolutions suggest that advanced information technologies have ushered in new ways of fomenting and effectuating political change.[1] On the other hand, when the crisis in Egypt escalated, the Egyptian authorities quickly cut internet access, mirroring the earlier actions of Iran in blocking access to Facebook and other sites during

* Professor of Law & Director of the Intellectual Property, Information & Communications Law Program, Michigan State University College of Law

[1] *See, e.g.*, Tara Bahrampour, *In Syria, Protesters Push to End Decades of Isolation*, WASH. POST, Apr. 16, 2011, http://www.washingtonpost.com/world/inspired-by-neighbors-and-technology-syrians-join-in-revolution/2011/04/16/AF3JPjqD_story.html ("For decades one of the Middle East's most isolated societies, Syria has in recent years allowed its people access to the Internet and satellite television. Now, technology is playing a crucial role in their democracy movement, as Facebook, Twitter, YouTube and Skype help them evade government detection as they communicate with one another and disseminate information."); Robert Fisk, *But What If the Spirit of Rebellion Spread To Iran?*, THE INDEPENDENT (London), Apr. 23, 2011, http://www.independent.co.uk/opinion/commentators/fisk/robert-fisk-but-what-if-the-spirit-of-rebellion-spread-to-iran-2273779.html (quoting a tweet describing the Egyptian revolution as "organized by facebook, spread by twitter and organized by a guy working for Google"); Uri Savir, '*And the Young Shall Lead,*' JERUSALEM POST, Mar. 30, 2011, http://www.jpost.com/LandedPages/PrintArticle.aspx?id=214487 ("[W]hat made the revolutions in Tunisia and Egypt actually happen are two driving forces—the young generation and technology . . . . The full ramifications of the Internet revolution are not yet defined, but Cairo and Tunis proved that powerful change can happen through social media—change that affects social intercommunication and activities. Facebook has become a new superpower. . . ..").

the failed so-called "Green Revolution."[2] The 2010 State Department Human Rights Report explicitly states more than forty countries are blocking, controlling, or monitoring internet traffic in a morally offensive way.[3] From this perspective, information technologies simply empower governments to cling to power by monitoring and controlling their citizens.

The centrality of information technologies in recent political turmoil, and the State Department's interest in government control of internet traffic, shows that internet traffic constitutes political power. As Secretary of State Hillary Clinton states,

> The final freedom, one that was probably inherent in what both President and Mrs. Roosevelt thought about and wrote about all those years ago, is one that flows from the four I've already mentioned: the freedom to connect – the idea that governments should not prevent people from connecting to the internet, to websites, or to each other. The freedom to connect is like the freedom of assembly, only in cyberspace. It allows individuals to get online, come together, and hopefully cooperate.[4]

What is interesting from a regulatory perspective, as opposed to one that is normative or political, is that unlike the international mail system or even the old telephone network, internet traffic routing is opaque. In the past, comprehensive government regulation made fairly precise information about telephone infrastructure within the United States available, and international treaties accomplished much the same for international traffic.[5] In other words, in distinction to predecessor networks, internet transparency is not a transparent regulatory concept.

If, in the words of Secretary of State Clinton, there is an internet "freedom to connect," such freedom implicates a knowledge or transparency about *how* internet interconnection works. After all, if your network degrades or blocks your messages secretly, no such freedom

[2] Amy Lee, *Egypt's Internet Shut Off—But How? The Blackout Explained*, THE HUFFINGTON POST, Jan. 28, 2011, http://www.huffingtonpost.com/2011/01/28/internet-egypt-shut-off_n_815495.html#s232525&title=Nick_Ellis; Associated Press, *Iranian Activists Search For Ways to Defy Internet Restrictions*, FOXNEWS.COM (July 24, 2009), http://www.foxnews.com/story/0,2933,534773,00.html.

[3] U.S. STATE DEP'T, INTRODUCTION, 2010 COUNTRY REPORTS ON HUMAN RIGHTS 1, 3, *available at* http://www.state.gov/g/drl/rls/hrrpt/2010/frontmatter/154329.htm.

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

[5] *See infra* Part I for a discussion of transparency in the U.S. domestic telephone network and international interconnection.

could exist. The purpose of this essay is to identify the challenges in creating internet disclosure on an international level. Even if a strong argument can be made that internet transparency is a central legal, political, and even human rights issue,[6] bureaucratic ukase cannot easily define or mandate internet transparency.[7] It is a remarkably complex matter.

As an initial distinction, internet transparency refers to different concepts. "Private network transparency" refers to the so-called network neutrality or network openness debate.[8] This cluster of issues involves private actors, such as private broadband service providers, working within their own network, discriminating against certain types of network traffic. Their motivation can be network efficiency and optimization—or content discrimination for economic reasons—or a possible combination of both.[9] For example, Comcast, unbeknownst to customers, blocked peer-to-peer ("P2P") traffic. Comcast claimed it did so to maximize network performance while others claimed an anticompetitive effort to slow P2P sharing, possibly to protect its own video delivery business.[10]

What bothers the State Department, however, is not "private transparency" but "public network transparency" (*i.e.,* political and state actors blocking or monitoring politically undesirable traffic).[11] This essay compares "private transparency" (*i.e.,* the difficulty of under-

[6] Many others have examined the human rights aspect of the internet and realized the importance of disclosure and transparency. *See* Milton Mueller, *Timid liberalism: A critique of the process-oriented norms for Internet blocking, in* TRANSNATIONAL CULTURE IN THE INTERNET AGE: NEW PARADIGMS FOR LAW & COMMUNICATIONS (Sean A. Pager & Adam Candeub eds., forthcoming 2012); Derek E. Bambauer, *Cybersieves*, 59 DUKE L.J. 377, 393-96 (2009).

[7] This normative notion—that network transparency is a human right predicated on free speech—deserves extensive treatment. *See* Adam Candeub & Daniel John McCartney, *Law and the Open Internet*, FED. COMM. L. J. (forthcoming 2011). This article is concerned with the regulatory challenges involved in network transparency and will leave to another time a defence of the concept.

[8] *See* Adam Candeub & Daniel John McCartney, *Network Transparency: Seeing the Neutral Network*, 8 NW. J. TECH. & INTELL. PROP. 228, 228-29 (2010).

[9] *See id.* at 229 (stating that some networks block spam or malware); Formal Complaint of Free Press and Public Knowledge Against Comcast Corp. for Secretly Degrading Peer-to-Peer Applications, 23 F.C.C. Rcd. 13028, ¶ 5-9 (2008) (memo, opinion and order) (describing how Comcast blocked peer-to-peer applications that competed with its video-on-demand services).

[10] Formal Complaint of Free Press and Public Knowledge Against Comcast, 23 F.C.C. Rcd.at 13055.

[11] U.S. STATE DEP'T, *supra* note 3, at 3.

standing traffic flow due to the commercial and contractual nature of internet interconnection) with "public transparency" (*i.e.*, efforts, such as those of China or Saudi Arabia, to control and monitor traffic via direct government action).

Finally, this essay argues that some sort of legal or policy response is necessary to further public and private network transparency. That said, it is not clear what these efforts might include because of (i) the difficulty of reducing transparency to a few, easily understandable metrics and (ii) the secrecy that shrouds private internal network management, peering agreements, as well as government monitoring and blocking efforts. This essay argues that transparency can best be achieved at the wiki level (*i.e.*, individuals using the nature of the internet itself to understand its interconnection and traffic routing). Once again, in marked distinction with predecessor networks, such as telegraphy and telephony, the internet allows individuals to track and uncover behavior in ways previously inconceivable. Numerous scholarly and policy groups are working to uncover internet workings.[12] Such efforts are at their infancy, or at least childhood, and law and public policy can support such efforts.

I. The Challenge of Internet Transparency and the Old Days

The telephone network was, at least in its early iterations, purely circuit based. That means that there was an electrical circuit opened between the calling and called party. That circuit was opened at the switch, which was nothing but the place at the central office where the telephone wires converged.[13] The operator, as the old movies attest, connected end users manually. She would do this by physically inserting cables into a switchboard.[14]

These circuits were identifiable in both a physical and legal, regulatory sense. The switches were physically present at easily identifiable central offices, and the Federal Communications Commission ("FCC") oversaw domestic interconnection between telephone companies.[15] Due to its ratemaking regulation, the FCC kept exhaustive information about the physical plant, which determined where traffic flowed. If

[12] *See infra* Part III.

[13] Hill Assocs., Telecommunications: A Beginner's Guide 5-9 (2002).

[14] And it was "she." AT&T made it a policy to hire female operators. *See* Venus Green, Goodbye Central: Automation and the Decline of "Personal Service" in the Bell System, 1878-1921, 36 Tech. & Culture 912 (1995).

[15] Hill Assocs., *supra* note 13, at 5, 27.

you made a call from Des Moines to New York City, the FCC knew the circuit on which the call travelled.[16] More importantly, regulation mandated quality of service. Thus, a telephone company could not discriminatorily degrade traffic to any customer or group of customers.[17]

From an international perspective, treaty and international agreements determined telephone interconnection. At least originally, government treaty determined the telephone interconnection point and the terms under which traffic was exchanged.[18] If someone in New York wanted to call Paris, the wires over which circuit the call travelled would be easily identifiable. Again, terms and conditions of traffic exchange were transparent and, indeed, largely standardized through the work of the International Telecommunications Union.[19]

In short, transparency in the old telephone network was relatively easy. When a private party—or for that matter a government—wanted to block or degrade traffic, it was obvious and illegal, without a warrant or analogous special legal permission.

II. The Internet and Transparency

Compared to the international mail system or even the telephone network, internet networks do not exchange information using discrete circuits. Rather, information is digitized, spliced into bits and pieces, and can be sent through myriad different internet routers throughout the world. The information is addressed so that routers know how to transfer the traffic, but unlike telephone traffic, one cannot predict what physical lines this information will travel. The routers only "know" about their immediate network environment. Bits of in-

[16] *See generally* Richard Gabel, Development of Separations Principles in the Telephone Industry 35-45 (1967).

[17] The obligation to not discriminate, though not absolute, permeated telephone regulation. *See* Adam Candeub, *Network Interconnection and Takings,* 54 Syracuse L. Rev. 369, 393 (2004).

[18] Peter F. Cowhey, *The International Telecommunications Regime: The Political Roots of Regimes for High Technology,* 44 Int'l Org. 169, 169 (1990).

[19] *See id.* at 175 ("The point-to-point nature of international telecommunications traffic (a telephone call goes, say from New York to London) encouraged bilateral coordination among governments, particularly where there was heavy traffic flowing over cables. But unless bilateral agreements were covered under a multilateral umbrella, they could easily have contradicted each other, hampered instead of encouraged the international flow of communications, and been subject to competitive end runs. Therefore, global coordination was simplified when a set of umbrella rules and standards was negotiated multilaterally.").

formation sent from one user to another can travel all over the world. The internet protocols do not permit one to discover the information's path.[20]

The challenge, therefore, of making the internet transparent is three-fold. First, disclosure must show how broadband service providers manage their own network (*i.e.,* the upload/download rates, the differential treatment of types of traffic, etc.). Transparency is essential to determine when differential treatment could have an anticompetitive incentive or effect, as with the BitTorrent-Comcast controversy discussed below.[21] Second, the way broadband providers interconnect, and the registries they use for their traffic, are essential in determining how internet traffic flows. Backbones typically exchange traffic in secret bilateral agreements, creating a vast global network that interconnects under terms which no single entity knows.[22] (This situation is somewhat alleviated by some of the quasi-public requirements of peering points.) Third, and most importantly from a political perspective, are government efforts to block and control internet traffic.[23] Government blocking can be accomplished in a variety of ways that appear to employ both selective interconnection and internal management techniques. For instance, the famous "great wall" of China employs selective interconnection (all of China interconnects to the internet at one point) and internal management (undesirable sites, and search terms, are blocked).[24]

Given these complexities, internet "transparency" is not a transparent concept. Internal network management involves complex com-

[20] This is hardly the place to provide a description of the way the internet functions. For this essay's purposes, it is simply important to realize that traffic does not travel over distinct, identifiable paths. For a useful, non-technical description of internet traffic, see TELECOMMUNICATIONS: A BEGINNER'S GUIDE, *supra* note 13, at 226-30.

[21] *See* Adam Candeub & Dan McCartney, *Network Transparency: Seeing the Neutral Network,* 8 NW. J. TECH. & INTELL. PROP. 228, 235 (2010) (discussing how the BitTorrent-Comcast controversy provides an example of how differential treatment may create an anticompetitive incentive).

[22] *See id.* at 229 (emphasizing the confusion created by the secrecy of backbones in the past).

[23] *See* OpenNet Initiative, *2010 Year in Review, available at* http://opennet.net/about-filtering/2010yearinreview (last visited July 30, 2011) (stating that the 2010 Year in Review provides "a summary of events worldwide concerning the practices and policies of Internet content filtering, surveillance, and information warfare.").

[24] *See, e.g.,* Steven J. Murdoch & Ross Anderson, *Tools and Technology of Internet Filtering, in* ACCESS DENIED: THE PRACTICE AND POLICY OF GLOBAL INTERNET FILTERING 5, 11 (Deibert, R. et al. eds. 2008).

puter protocols and routing techniques. Backbone interconnection involves secret bilateral contracts in which backbones promise each other a certain quality of service. Additionally, there is the specter of government monitoring and possibly traffic control, about which very little is publically known. The following explores these complexities in greater detail, spelling out why internet transparency is such a difficult goal to achieve.

A. *Internal Network Management*

All networks optimize, using limited network resources to provide the best service possible. Inevitably, this involves treating some types of traffic differently than others. For instance, some traffic, such as streaming video, can tolerate less delay than email. Giving "priority" to streaming video allows people to watch videos without "jitter," but the same priority need not be given to email, as a delay of one to two seconds for email delivery can hardly be noticed.[25]

But treating different types of traffic differently can have less benign motivations. For instance, it was alleged that Comcast's blocking of P2P traffic was an effort to block sharing of movies, which of course compete (in a rather attenuated way) with Comcast's video service. This type of anticompetitive activity motivates the so-called network neutrality controversy.[26]

Moving away from economics, internal network management regimes can have political implications. For instance, several years ago Verizon refused a request from the abortion rights group, NARAL Pro-Choice America, for a five-digit "short code." Verizon routinely gave short codes to businesses, politicians and advocacy groups. These codes allow interested individuals to sign up to receive regular text messages.[27]

While a public outcry forced Verizon to quickly drop its "anti-abortion regime," the episode illustrates the power of broadband providers, in theory, to block politically undesirable traffic. For the reasonably paranoid, such power raises questions given how enmeshed the telecommunications sector is with the government. These concerns

[25] *See* Candeub & McCartney, *supra* note 21, at 232-34.

[26] *See id.* at 235-36 (describing how the anticompetitive activity in the BitTorrent-Comcast controversy contributes to the network neutrality controversy).

[27] Adam Liptak, *Verizon Reverses Itself on Abortion Messages*, N.Y. TIMES, Sept. 27, 2007, *available at* http://www.nytimes.com/2007/09/27/business/27cnd-verizon.html.

are not abstract. For instance, in the uproar that followed 9/11, President Bush authorized the Terrorist Surveillance Program, which included government wiretapping without warrants.[28] The Bush Administration admitted that it coordinated with the large telecommunications companies in illegal searches.[29] Lawsuits that were filed came to nothing because Congress granted the telecommunications companies legal immunity.[30] Companies that need (and in fact receive) statutory legal immunity from Congress likely lack immunity from the political pressure affecting the management of their networks.

Thus, some internal management regimes are inherently discriminatory, but it is difficult to distinguish "good" from "bad" discrimination.[31] Even more basically, however, it is a challenge to specify internal management regimes. Unlike the telephone network's quality of service, internet quality cannot be reduced into a few, simple, easily understood metrics.[32] Effective disclosure must actually aid markets in developing information and in assessing the value and quality of internet access, but this proves to be very tricky.

First, no one entity has the incentive to produce complete information about any one user's internet quo.[33] This is because the scattered infrastructure owners have their own discrimination policies and only know the identity of their set of adjacent peers.[34] Even though one could estimate an internet service provider's ("ISP") value using a recursive function (such as the sum of the value of their peers, re-

[28] *See* James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. Times, Dec. 16, 2005, at A1, *available at* http://www.nytimes.com/2005/12/16/politics/16program.html ("Months after the Sept. 11 attacks, President Bush secretly authorized the National Security Agency to eavesdrop on Americans and others inside the United States to search for evidence of terrorist activity without the court-approved warrants ordinarily required for domestic spying . . . .); *see generally* Zachery Keller, *Big Brother's Little Helpers: Telecommunication Immunity and the FISA Amendment Act of 2008*, 70 Ohio St. L.J. 1215, 1219-28 (2009).

[29] Eric Licthblau, *Role of Telecom Firms in Wiretaps Is Confirmed*, N.Y. Times, Aug. 24, 2007, at A13, *available at* http://www.nytimes.com/2007/08/24/washington/24nsa.html ("Under the president's program, the terrorist surveillance program, the private sector had assisted us, because if you're going to get access, you've got to have a partner[.]").

[30] *See* 50 U.S.C. § 1885a (Supp. II 2008); Keller, *supra* note 28, at 1232-33.

[31] Kevin Werbach, *Only Connect*, 22 Berkeley Tech. L.J. 1233, 1280 (2007) ("Regulators will have a difficult time determining if such algorithms are motivated by legitimate network management concerns or anti-competitive impulses.").

[32] *See* Candeub & McCartney, *supra* note 21, 231-34.

[33] *Id.* at 231.

[34] *Id.*

duced by the aggregate traffic discrimination among those peers), the ISP cannot be expected to disclose the traffic policies of all its peers, and of all their peers' peers, and so on. This would amount to a single ISP disclosing the network policies of the entire accessible internet. It is not clear that any one ISP would have the ability, let alone incentive, to acquire the information to do so.[35]

Second, the technical complexity of extensive disclosure will render such disclosure of little use to the typical consumer. Like the disclosure on prescription drugs—those inserts with detailed information about the composition and chemical attributes of the accompanying drug for which an advanced degree in pharmacology is required to understand—technical disclosures of traffic management and peering relations cannot provide guidance to the average consumer.[36]

B. *External Interconnection*

Once internet traffic leaves a broadband service provider's network, it enters the backbone, the complex global network of fiber optics that transfers all internet data. Bilateral contracts determine the relationship between broadband providers and the backbone, as well as between backbones. These relations specify at what price, if any, a backbone will carry another backbone's traffic. They also specify at what quality traffic will be carried. These agreements are generally secret.[37]

Alternatively, backbones can connect at internet exchange points or "IXPs." These are nodes at which multiple carriers exchange traffic. Sometimes they have standard (and published) rules for traffic exchange. Other times, they simply provide the physical location at which interconnection occurs, and parties work out the terms of interconnection.[38]

The challenges for disclosure are large and obvious. These agreements are largely secret, and absent government intervention—*on a*

[35] *Id.* at 234 n.16 ("Also the ISP's peering relationships are not meaningful without reference to the topography of the rest of the Internet; an ISP cannot be expected to know this topography let alone to disclose it to the consumer over the phone. Instead, there must be a bridge to close the gap between users who are positioned to signal their preferences and the meaning of the technical information that an ISP discloses.").

[36] *Id.*

[37] *See id.* at 231-37.

[38] *See generally* Alessio D'Ignazio & Emanuele Giovannetti, *Asymmetry and discrimination in Internet peering: evidence from the LINX*, 27 INT'L J. INDUS. ORG. 441 (2009).

global scale—no one will be able to provide a complete picture of internet traffic flow. Quality of service is additive. As traffic is handed from the broadband provider to backbone to provider, each network's internal network management, as well as the terms of its interconnection agreements, affect any given end-user's internet experience.

C. *Political Blocking*

The recent unrest and revolution in the Mideast underscore both the essential nature of the internet for modern political discourse *and* the political importance of network transparency. Facebook and wireless technology played a key role in organizing the opposition movements in Iran and later in Egypt.[39] Citizens in numerous other countries used this model.[40]

At the same time, governments responded by blocking the internet. Iran blocked Facebook and Egypt simply "turned off" the internet. Interestingly, in both situations, there was limited success. Egypt left one ISP in operation because the stock market depended on it. Egypt could not block dial-up traffic because to do so would require turning off the telephone network.[41] In Iran, the use of proxy addresses allowed continued access to Facebook, at least for the technologically clever.[42]

Countries with longer term political control issues have developed more complex and comprehensive approaches. For instance, Saudi Arabia, like many other countries, simply blocks sites. China takes a more complex approach, apparently monitoring and blocking traffic at the level of search terms. The Chinese government, therefore, can monitor content within search terms, emails, and text messages.[43] The

[39] *See, e.g.*, Brad Stone & Noam Cohen, *Social Networks Spread Defiance Online*, N.Y. Times, June 16, 2009, at A11, *available at* http://www.nytimes.com/2009/06/16/world/middleeast/16media.html.

[40] *See* Freedom on the Net 2011: A Global Assessment of Internet and Digital Media 3 (Sanja Kelly & Sarah Cook eds., Freedom House 2011).

[41] *See* Christopher Beam, *Block Like an Egyptian: How did the Egyptian government turn off the Internet?*, Slate, Jan. 28, 2011, *available at* http://www.slate.com/id/2283000/; *see* Matt Richtel, *Egypt Cuts Off Most Internet and Cell Service*, N.Y. Times, Jan. 28, 2011, *available at* http://www.nytimes.com/2011/01/29/technology/internet/29cutoff.html?_r=1.

[42] *See, e.g.*, Iran-Proxy Discussions, http://www.facebook.com/board.php?uid=122958306978&f=2&start=30&hash=3158abad95f26ac25be99c263ae68775 (providing advice on how to set up proxy Facebook accounts).

[43] *See* Freedom on the Net 2011, *supra* note 40, at 4 ("Keyword filtering is much more nuanced, enabling access to a given website but not to a particular article containing a sensitive keyword in its URL path. Among the countries studied, China, Iran, and

2010 State Department report, as well as other sources, describe a bevy of strategies that countries have developed to monitor the internet and control routing.[44]

The barriers to disclosure of the nature of this blocking are, of course, obvious. Nations by definition want to keep *how* they monitor and block traffic secret. Knowledge of this monitoring is only accomplished when users cannot reach sites—or, in the case of keyword monitoring, when the police come knocking.

III. Conclusion: Building Internet Transparency

The barriers to true internet transparency—the difficulties of specifying an effective disclosure due to the complexity of routing and network management, the decentralization of interconnection agreements, and, finally, government control—seem insurmountable. But what can regulation do, if anything?

At a national level, much can be done. Internet disclosure can be mandated. The recent landmark "network neutrality" decision by the Federal Communications Commission declined to impose standardized disclosure.[45] Rather, it recognized the importance of disclosure and mandated disclosure of network management protocols but did not specify the form. Whether these disclosures will be effective without standardization is not clear. The FCC wisely promised to "continue to monitor compliance with this rule, and may require adherence to a particular set of best practices in the future."[46] This is certainly a move in the right direction. National regulatory agencies can and must do more to create norms and expectations concerning internet transparency.

At an international level, law can do less. There is no entity that could compel the multitude of actors, private and governmental, to provide adequate data. The best that can be done is what Hillary Clin-

Tunisia are known to have such systems in place. In China, which boasts the world's most comprehensive censorship apparatus, keyword filtering is evident in instant-messaging services as well, having been built into the software of popular messaging programs like TOM Skype and QQ.").

[44] *E.g.*, U.S. State Dep't, *supra* note 3.

[45] In the Matter of Preserving the Open Internet Broadband Industry Practices, 25 F.C.C. Rcd. 17905, 17939-41 (2010) (refusing to impose standardized disclosure but promising to monitor the situation closely). *See generally id.* at 18001 (citing comments of Adam Candeub & Daniel John McCartney).

[46] *Id.* at 17940.

ton is doing as evidenced by her previous quotation: use international pressure and persuasion to create norms and expectations concerning internet access and transparency.[47]

Yet, before we despair of doing anything, it seems at least possible that the internet itself offers a way forward. Unlike the predecessor telephone system, internet networks offer end-users the ability to learn about its workings. The internet's "end-to-end" distribution of functions allows creative users to develop computer tools that learn *how* the internet works. Indeed, there are many such examples.

Numerous private efforts are providing useful disclosure about internet traffic flows. On private internet transparency, the Electronic Frontier Foundation recently made the first release of its "Switzerland" software, which examines internal network management. As Candeub and McCartney explain:

> Switzerland lets users explicitly coordinate with a trusted third party to validate traffic. It detects any drop, forgery, or modification between any two computers, when both are running the software. It also tracks a variety of meta-data about the quality of the connection, in hopes of someday detecting more subtle interference.[48]

To infer external interconnection between and among networks, groups such as the Cooperative Association for Internet Data Analysis (CAIDA) developed a tool named "skitter" to collect this traceroute data from twenty-five strategically placed locations around the internet.[49] As for public transparency, researchers at the OpenNet Initiative, a collaboration among the Citizen Lab at the University of Toronto, the Berkman Center for Internet & Society at Harvard Law School, and the SecDev Group (Ottawa),[50] have developed software to measure and detect government tampering and monitoring of internet traffic.[51] These imperfect efforts are in their infancy but promise a "netroots" response to infringements, both public and private, on the "freedom to connect."

[47] *See* Clinton, *supra* note 4; *see also* Mueller, *supra* note 6.

[48] Candeub & McCartney, *supra* note 21, at 237.

[49] *Id.* at 238.

[50] *See* OpenNet Initiative, http://opennet.net/ (last visited Aug. 23, 2011).

[51] *See, e.g.,* Robert Faris & Nart Villeneuve, *Measuring Global Internet Filtering, in* ACCESS DENIED: THE PRACTICE AND POLICY OF GLOBAL INTERNET FILTERING 5, 11 (Ronald Deibert et al. eds., 2008).

To the degree the international community believes that the "freedom to connect" is a basic human right, it must support efforts to discover *how* the internet connects. Without such knowledge, any such right is illusory.