Intersect, Vol 8, No 2 (2015)

An Investigation of Decentralized Networks Based Upon Wireless Mobile Technologies

Haley Lepp
Georgetown University

Abstract

The Internet is a highly centralized and hierarchical structure that leaves users with a number of potential barriers to connectivity. As wireless networking becomes more common and mobile devices grow in popularity, a variety of decentralized networks have emerged to break down or create alternatives for connectivity barriers. These mesh-like networking options work either as extensions of traditional Internet infrastructure or simply as inward-facing user networks. This paper explores the various impediments that these networks seek to circumvent: namely, economic barriers to connectivity, unintentionally destroyed infrastructure, intentionally blocked infrastructure, and government surveillance. After a careful analysis of the goals these networks aim to achieve, it is clear that networks that attempt to solve problems caused by centralization often succeed, while users seeking other functionalities are often disappointed.

I. The Problem of Centralization: "If you thump it on the head, will it die?"

Centralized structures are, by nature, vulnerable. When the entirety of a structure relies on one central head, if anything happens to that central head, the rest of the structure collapses. Additionally, because anything seeking to destroy the structure simply needs to destroy the center, the center becomes a target for destruction. In their book, *The Starfish and the Spider,* Ori Brafman and Rod Beckstrom compare the model of a spider, a centralized structure, to that of a starfish (Brafman & Beckstrom, 2006). When thumped on the head, a spider ceases to function. A starfish, however, does not have this vulnerability; with no "head," there is no simple "node" to disconnect that will disable a starfish. Even if the legs of a starfish are cut off, new legs will grow back. The infrastructure of the Internet resembles a spider; this centralization presents a number of vulnerabilities.

The Internet, as it exists today, functions as a network of centralized networks. To become part of one of these networks, computers or mobile devices must somehow access an Internet Service Provider (ISP) either by

direct connection or through a local area network (LAN) or wireless LAN (WLAN). By connecting to an ISP, the device, or smaller network of devices, becomes an outer node of that ISP's network. While individual users can pay to connect to most ISPs, different ISPs have different levels of connectivity. Small, local Tier-3 ISPs pay to connect to regional Tier-2 ISP networks, which pay to connect to much larger national and international Tier-1 ISP networks (Center for Applied Internet Data Analysis [CAIDA], 2014). ISPs are generally considered to be Tier-1 if the provider can reach all other networks simply by using Internet Exchange Points (IXPs) without paying other ISPs for access. IXPs, either run commercially or through public sectors, are physical network access points, often made of massive fiber optic cables, where ISPs exchange traffic (Jensen, 2009). IXPs serve as the top level of the Internet's topology; they are the only way in which Tier-1 ISPs can connect, and thereby create the backbone of the broader Internet (OECD, 2014).

The Internet's highly hierarchical topology presents a number of vulnerabilities to worldwide connectivity. ISPs, which have continued to merge over the last decade, are decreasing in number and therefore hold an immense amount of control over their user bases (Brodkin, 2014). ISPs can and have leveraged that control as a source of market power, using monopolistic business practices to keep prices high and competition low (Cassidy, 2014). As a result, connectivity continues to be a luxury good, only available to those who can afford to pay for expensive contracts. Limited access as a result of poverty can occur either by the choice of consumers or at a corporate level: ISPs can choose not to build infrastructure in low-income areas, from underserved communities in the United States to developing countries. This phenomenon is generally referred to as the Digital Divide, and has been widely researched as a contributor to the growing gap between rich and poor around the world (Goodman, 2013).

The Internet's hierarchical topology can also serve as a security vulnerability: ISPs and IXPs have proven popular targets for actors aiming to decrease or control connectivity. For example, in 2011, when Egypt experienced mass protests, the Mubarak regime successfully targeted the Cairo Internet Exchange (CAIX) as a way to control citizen Internet access (Singel, 2011). CAIX, which serves as an exchange point for most major ISPs in Egypt, including Vodafone, Link, Telecom Egypt, and Etisalat Misr, is one of only two IXPs in Egypt and most, if not all, of Egypt's fiber optic circuits go through its location at Ramses Exchange (Cairo Internet Exchange, 2014). Due to this centralized structure, the Egyptian government was able to take down 93% of the country's Internet access in only 28 minutes (Cowie, 2011) simply by flipping a "kill switch" at the Ramses Exchange IXP (Glans and Markoff, 2011) and ordering the four major Egyptian ISPs to shut down their networks (Vaas, 2012). By knocking out the top of the country's Internet hierarchy, the regime quickly caused a countrywide Internet outage (Johnson, 2011). Until the

Egyptian shutdown, censorship by authoritarian regimes took milder forms, such as the blocking of specific websites: a total shutdown was unheard of. For this reason, the Egyptian shutdown has served both as a warning to the international community that intentional total blackouts are possible and apparently tenable. The Egyptian shutdown has also acted as a model of censorship for authoritarian regimes attempting to maintain stability.

Alternatively, access can be limited unintentionally due to physical damage resulting from natural disasters. During Hurricane Sandy in 2012, customers up and down the east coast lost connectivity, and users around the United States lost access to certain sites. Regional ISPs had various explanations, including flooded data centers, disrupted cables, and electricity outages (Reardon, 2012). Because Internet users and media outlets around the United States rely on only a few major nodes to connect, a storm physically affecting only the Northeast drastically damaged connectivity around the entire country (Reardon, 2012).

II. The Emergence of Decentralized Networks in a Mobile, Wireless Society

Networks that resemble starfish and do not rely on centralized hierarchical topologies have long existed in a range of technologies. The Institute of Electrical and Electronics Engineers (IEEE) published a paper in 2005 highlighting the market potential of MANETs, or mobile ("multi-hop") ad hoc networks, and an emerging class of networks called "mesh" networks (Bruno & Conti, 2005). A MANET is a collection of mobile nodes that freely organize into "arbitrary and temporary ad hoc network topologies" instead of the typical hierarchical Internet topology (Bruno & Conti, 2005). Such a network does not require any preexisting infrastructure. Instead, the network relies simply on users' devices, which act not just as terminals, but also as routers for other devices in the network. A mesh network, according to the IEEE paper, is a MANET that relies on at least one fixed node that connects to the greater Internet; the mesh network thus acts not as a parallel self-contained network of users, but as an extension of wired infrastructure networks. The IEEE paper recommends that "mesh networks" be developed as a way to provide public outdoor connectivity to roaming users (Bruno & Conti, 2005).

In September of 2013, Apple introduced a mesh-like capability in iOS7 called Multipeer Connectivity Framework (Ou, 2014). This framework was designed to allow all of a user's devices to simultaneously communicate in a peer-to-peer fashion instead of through a common node. For example, with this framework, an iPad and an iPhone can communicate directly, even if no existing connection to the greater Internet exists. Such a framework gives users immense flexibility, and therefore security in connectivity. Whether all devices are connected directly to a Wi-Fi network, only one device is connected directly, or none

of the devices connect to the network, the devices themselves can still connect via Bluetooth (Anthony, 2014).

The decentralized networks envisioned by the IEEE researchers and Apple developers have, in the last five years, proven to be successful in ways beyond their original intentionality. Users around the world have adopted the decentralized networks to counteract the vulnerabilities created by the centralized structure of the Internet. These emerging decentralized networks have been able to provide solutions to vulnerabilities by taking advantage of two powerful new resources: the widespread use of wireless devices and the rise of smartphone usage around the globe. Prior to the rise of wireless devices, the centralized topology of the Internet was practical. A user, for example, could not have direct connections to all the other devices she wanted to reach (that would be a lot of wires); instead, she only needed one link, to her ISP, who would then connect her to other users. With the more advanced wireless technology now common in every-day devices, it is possible for users to connect directly to other users in proximity to them without going through an ISP. Additionally, the rise of mobile device usage around the world has led to the closer proximity of devices. With more devices close enough to make direct connections, "multi-hop" linkages can grow: User A, aiming to connect to a far away User C, can connect to man-in-the-middle User B's device. User B then will connect to User C to share data. Before the advent of the wireless mobile technology age, all three users needed to connect to an ISP in order to communicate.

The decentralized networks that have emerged in recent years share a basic structure: each device, or node, in the network is connected to every other node around it (Rouse, 2014). When a device sends data, the data "hops" along a chain of nodes until it reaches the intended receiver (Skaar, 2014). In sophisticated networks, the originating node will send only a small amount of data until the most efficient route is established. As nodes do not rely on a central connecting point, the network is self-repairing; traffic routes and reroutes through the many possible linkages instead of failing if one node loses a connection. Hypothetically, such a network increases in strength as it grows. Because each additional node acts as a router, more nodes create more potential routes for transmission. This redundancy then reduces the effect of a single node failure (Skaar, 2014). Some networks, depending on intended purpose, use key encryption to ensure privacy and security, while some networks do not encrypt messages, instead using the network as a sort of "megaphone" to spread a single message to a large group (Meyer, 2014).

Though they share similar structures, decentralized networks differ in functionality. A number of networks around the world, for example, serve to provide an alternative to expensive or discriminating ISP service. Guifi.net, a wireless community network that primarily exists in Catalonia, was developed in the early 2000s to bring Internet connectivity to rural regions where ISPs did not have established infrastructure (Finch, 2013).

Networks have been attempted for similar purposes in underserved areas in the United States, including Detroit and Pittsburgh. Other networks have been developed to serve as temporary solutions to unintentionally destroyed infrastructure: Red Hook, a community network in Brooklyn, received media attention by bringing connectivity to aid workers and victims of Hurricane Sandy (Kazansky, 2012). Similar temporary solutions have appeared internationally as a result of intentionally blocked or destroyed infrastructure: mesh networks in Tunisia, Egypt, and the Sudan provide alternative means of communication to populations who face either total Internet shutdowns or partial censorship. Finally, in the last year, there have been attempts to use mesh networks as a way to bypass surveillance and maintain user privacy. Open Garden, a Silicon Valley-based startup, has made international news with its potentially disruptive new mobile application, Firechat. Users around the world have downloaded Firechat to create networks to bolster existing infrastructure, bypass shutdowns, or avoid surveillance. Some of the networks listed have enjoyed immense success, while others have failed to achieve their users' intentions. In the following pages, I will analyze the development of decentralized networks for these different functions, and determine in which environments they can provide solutions, and in which they cannot.

III. Bridging the Digital Divide: Guifi and Cass Corridor

One of the most inhibiting consequences of the ISP-centered Internet structure is its contribution to the Digital Divide. The Digital Divide refers to the growing economic gap between telecommunications have and have-nots – a divide that can determine the ability of an individual or a community to achieve a level of income necessary for a high quality of life (Goodman, 2013). The monopolistic practices of ISPs around the world contribute to the Digital Divide in two significant ways. First, commercial ISPs choose to invest infrastructure in high-income areas where high profits can be gained from large, affluent consumer populations. ISPs often neglect to provide service in areas with low-density or low-income populations. Second, even in areas in which commercial ISP infrastructure exists, exorbitantly high prices provide barriers to many potential users who cannot, or choose not, to pay for service (Brown, 1995). Because of the economic consequences that can result from lack of connectivity, many populations that do not hold contracts with commercial ISPs, along with activists, local governments, and social justice groups, have developed a variety of decentralized communication networks to meet unmet connectivity demand.

Guifi.net is an international "Community Wireless Network" (CWN) that advertises its services as "open, free, and neutral" to any user who seeks to join. As of the writing of this paper, the network hosts over 26,000 operating nodes with almost 42,000 total nodes (Guifi.net, 2014). The network was started in 2004 as a citizen initiative in Osona, a region of Catalonia, Spain, where a lack of commercial broadband infrastructure

left most of the population unconnected (Oliver, Zuidweg, & Batikas, 2010). While Osona is home to over 100,000 people, the population is spread throughout extremely small, rural villages, leaving ISPs little incentive to build up infrastructure in the region. For this reason, Guifi quickly received financial support from local municipalities that sought a cost-efficient solution to cover these distances and reach rural homes (Oliver, 2010). The CWN did not seek to replace or compete with commercial ISPs: instead, the network complemented existing Internet infrastructure, covering "grey zones" in which commercial broadband access was limited (Oliver, 2010).

In recent years, Guifi has grown from its original rural focus. The network has established links in developing countries in Africa, Asia, and the Americas (Oliver, 2010). The network also hosts a broader demographic within Spain that has joined the CWN for reasons beyond limited infrastructure access. A significant part of the Catalonian population "feels a deep rooted resentment toward Telefónica," Spain's most prominent ISP, both because of the monopoly that Telefónica holds in Spain and because the ISP's services are priced much higher than other European broadband services (Oliver, 2010). As a free community-built network, Guifi presents an attractive alternative to commercial ISPs for disenchanted consumers.

In early 2013, the U.S. Department of State, inspired by the 2011 Egyptian Internet shutdown and the Detroit Digital Justice Coalition and aiming to strengthen local infrastructure, funded the creation of a similar community-centered project in Detroit, Michigan (Gall & Glanz, 2014). The need for a community network in southwest Detroit was clear. According to a Press Release from the New America Foundation's Open Technology Institute, the organization that helped to create the network, more than half of Detroit residents do not have Internet service at home "due to the cost of service and lack of investment in infrastructure by Internet service corporations" (The New American Foundation, 2012). This divide in service appears to follow racial boundaries; in 2004, only a third of African Americans surveyed in Detroit claimed to have home Internet connections (Baker & Coleman, 2002), compared to almost 65% of Americans at the time (International Telecommunications Union, 2013). To bridge this digital divide, the Open Technology Institute deployed a 20-node test network and "Digital Stewards" training program in the Cass Corridor neighborhood of Detroit. The Cass Corridor Network aims to provide the area with a way to share local information "about community meetings, public safety, an elder's health, environmental injustices, and industrial accidents" (The Cass Corridor Network, 2014).

The Cass Corridor Network is based upon Commotion Wireless, a free and open source software employed around the world by organizations experimenting with decentralized networks. The software, which connects devices in a decentralized structure, boasts dynamic routing capabilities, developed security features, and useful applications

that create both a way for users to distribute Internet access and a way for users to communicate within the network without an Internet connection (Commotion, 2014). To ensure that this network is truly decentralized - built by community members to suit their own needs - the Digital Stewards program trains community members as technologists and organizers to install nodes, guide "ecosystem" growth, troubleshoot, and train other community members (Gunn, 2013). The goal of the program, according to a recently trained septuagenarian community member, is not to give residents low-cost Internet (though this may be an added benefit): instead, the program's main motivation is to provide an underserved community with a tool to gather and spread information (King, 2012). Pittsburgh, Seattle, and Austin have attempted to implement similar networks. Though critics often measure success by the ability of mesh networks to replace ISPs, it is important to remember the original purpose of the networks: to provide connectivity where there previously was none (Bryum & Breitbart, 2013).

IV. Unintentionally Destroyed Infrastructure: Connectivity as Disaster Relief

In late 2011, community organizers in the Red Hook neighborhood of Brooklyn, New York asked the Open Technology Institute, the organization behind the Cass Corridor Project, to help develop a Red Hook CWN. While the Open Technology Institute did not have the resources available at the time to assist the Red Hook Community, the Institute connected Red Hook organizers with Alyx Baldwin,[1] a graduate student at Parsons School of Design who was developing mesh network platform for her thesis (Open Technology Institute, 2013). Baldwin's project, TidePools, acts as a localized mapping platform for Red Hook. TidePools is built like a game, a cross between the Sims and crisis mapping software, which presents a virtual, mapped-out model of the real-life Red Hook community (Valentine, 2014). Baldwin claims that she designed the software and Red Hook implementation not to explore the technical feasibility of mesh networks (which she claims is already well-established), but to build a platform from the ground up, with community members, for community members (Valentine, 2014).

Baldwin's project exhibited its true potential when crisis hit Red Hook. In fall of 2012, Hurricane Sandy devastated the neighborhood, flooding homes and commercial areas, taking out power and endangering lives. The CWN, which continued to function throughout the storm, provided a way for residents to alert people of their needs, to check up on their relatives, and to learn news of the outside world (Valentine, 2014). However, the CWN was not designed for heavy-wear: the network only had limited access capabilities. At any given time, the network could only

[1] On March 25, 2016, the following change was made: Jonathan Baldwin was changed to Alyx Baldwin. The relevant gender pronouns were also changed from he/him to she/her.

support between 100 and 150 connections (Valentine, 2014). In the days following the storm, the Open Technology Initiative developed a software for the community using SMS text messages and Google Geocoding API that allowed residents to text their location and needs to a contact number, which then mapped their information to TidePools. TidePools then hosted a discussion thread so that other community members and aid workers could respond to help requests (Valentine, 2014). FEMA, noticing the success of this network in distributing aid, provided a satellite link that connected to part of the Red Hook Network and installed another router on top of a nearby building (Simonite, 2013). While the satellite connection was only available for 30 days, provided only modest bandwidth, and had slow connectivity, the setup gave crucial connectivity to a population that desperately needed it. Following FEMA's lead, local ISPs also volunteered temporary gateways to the network (The Open Technology Institute, 2013). The Red Hook mesh network, then, in no way provided functionality parallel to existing Internet infrastructure. Instead, the community network served a purpose that highly centralized ISPs could not accommodate, acting as an extension of existing infrastructure to assist a particularly vulnerable consumer base.

V. Bypassing Intentional Blackouts: Alternative Routes to Connectivity in North Africa

Since the Mubarak regime shut down the Egyptian Internet to prevent the spread of massive public protests in late January of 2011, the vulnerabilities of centralized infrastructure have haunted users around the globe. Even during the blackout, Egyptians and international activists found innovative ways to escape the shutdown by bypassing traditional centralized infrastructure. Rumors abound of citizens using landline phones, fax machines, and radios to create dialup connections to modems outside of the country (The Daily Mail, 2011). Shervin Pishevar, an Iranian-born Silicon Valley entrepreneur, publicized the idea of a mesh network, and within hours of the shutdown launched the OpenMesh project, an attempt to create an alternative source of connectivity for disconnected Egyptians (Pishevar, 2011). International corporations also sought to assist users and thwart the ISP shutdown: Google and Twitter quickly announced a service that would allow users to tweet via voicemail and listen to voicemail tweets from others by calling one of three free international numbers (Kawamoto, 2011).

Other communities in North Africa also came up with creative ways to avoid extreme censorship and full or partial service shutdowns as authoritarian governments cracked down on Arab Spring protests. The Ben Ali regime, in Tunisia, for example, was notorious for strict regulations and filtering of Internet data (Open Net Initiative, 2014). Even after protests ousted the dictator, the Tunisian Agency of Internet, under direction of the military, continued to censor sites (Abrougui, 2011). To counter continued blocks to access, technologists and local government

authorities of Sayada, a small Tunisian city, created a CWN in late 2012. The network, based upon Commotion's software, blends the functions of a parallel network and an extension to Internet infrastructure in a unique style. The network is made up of twelve community routers situated on rooftops throughout the town and a number of community servers. The CWN gives users access to maps of Tunisia, 2,500 free books in French, Wikipedia in French and Arabic (synchronized with a Wikimedia site hosted in France), an application for document editing, and an application for chat and file sharing (The Open Technology Institute, 2014). The U.S. Department of State has provided $2.8 million in support of the project and has attempted to pursue similar projects in other countries with high Internet censorship (Gall & Glanz, 2014). It is unclear what the original goal was in creating this network; some sources suggest that the program's focus is to bring an inward-facing community network to an under-connected population. Others claim that the network was designed as a way for political dissidents who took part in the 2011 uprising to communicate more securely and freely. Regardless of the original intention, however, the network appears to serve both purposes.

Citizens in Sudan also came up with resourceful ways to remain connected during the Sudanese government shutdowns of 2013. Omar al Bashir's regime, following the example of Egypt's Mubarak, instigated a total blackout within Sudan as a way to deter the spread of massive popular protests (Madory, 2013). While protestors and Sudanese citizens struggled to combat government forces, the Internet blackout and extreme censorship of media sources prevented people from communicating and organizing. To break down these barriers, Khartoum based technologists built Abena, a program that takes advantage of working phone networks by connecting SMS messages to a crowd-mapping platform (Conley, 2013). Mohammed Hashim Saleh, a co-founder of Abena, explained that the program groups mapped events into categories: people killed, people detained, fires, demonstrations, and more. According to Saleh, these categories, organized onto a constantly updating map, are much more accurate and useful to citizens and international observers than exaggerated or censored statistics in state-controlled media (Sperber, 2013).

6. Attempts to Hide from Prying Eyes: Decentralized Networks to Avoid Surveillance

A number of Internet communities and application developers have attempted to create decentralized networks as a way to retain anonymity and avoid government surveillance. The popularity of these networks within the United States in the last few years may be a direct result of the NSA surveillance scandal and the proposals of several government anti-piracy measures. Reddit users, for example, have discussed since at least 2011 the potential of starting a new, alternative Internet, or "dark net." While the network never came to fruition, the users publicly debated the

potential of Tor, the Pirate Bay, Gnutella, and other networks that rely on peer-to-peer or friend-to-friend file sharing as ways to counteract government surveillance (Paul, 2011). A number of these privacy-seeking users have also joined community networks like Freifunk and Guifi to avoid prying eyes. However, to the dismay of these users, most, if not all, anonymizing networks have proven unsound against hackers and law enforcement.

A San Francisco-based startup has received international recognition in the last six months for its applications' capabilities against snooping governments. Open Garden, founded in 2011 by vocal net neutrality advocates to "provide free wireless broadband access to the Internet," has a number of applications that rely upon mesh networks (Crunch Base, 2014). The most prominent of these applications is the recently published FireChat, a messaging software that Open Garden advertises as a way for users to communicate "off the grid," regardless of Internet connectivity or phone service (iTunes Preview, 2014). With this feature, even the company cannot locate the user; for this reason, Open Garden cannot determine the number of people who use the feature (Lillah, 2014).

FireChat made international news when hundreds of thousands of protesters in Taiwan and Hong Kong adopted the application, fearing interruptions in cellphone or Internet service by the Chinese government (Cohen, 2014). While services were not, in the end, intentionally disrupted, the application served as a way for users to communicate when giant protesting crowds stressed cellphone networks (Cohen, 2014). The chat application has three modes: "everyone," a semi-global chat room, "nearby," which allows users in close proximity to chat over Wi-Fi, Bluetooth, or Apple's Multipeer Connectivity Framework, and "firechat," which organizes internet users into groups based upon themes (The Citizen Lab, 2014). The application also allows "anonymous" messaging, potentially giving protest organizers and participants a ground to voice opinions without worry of real-life government attention (Horwitz, 2014).

This "anonymous" mode has been popular with another population: Iraqis. At least 40,000 Iraqis downloaded FireChat during an Internet shutdown by the Iraqi government in early 2014. The Iraqi government, attempting to limit the coordinating power of Islamic extremists, blocked social media and mobile phone service, and later, instigated network outages. The application gave users a way to communicate around these outages (Smith, 2014). However, users in Iraq, like their counterparts in Southeast Asia, may have attributed more capability to the application than actually exists: FireChat does not create a "private internet," just as other community networks do not "foil digital spying"(Kuchler & Kerr, 2014). While it may prove extraordinarily difficult for a government to shut down an application like FireChat,[2] the application is not invulnerable

[2] While proponents argue that to take out a decentralized mesh network, every node must be destroyed, a network like FireChat could potentially be affected by radio jamming Bluetooth connections, for example.

to surveillance (Baraniuk, 2014). Though conversations within the mesh network are not visible from the outside, any user within the network can easily snoop on open chatrooms. FireChat also does not encrypt user information or messages, so users seeking protection from surveillance will have to look for other means of communication. The application succeeds in the actions it performs: allowing users to communicate when other methods of communication are unavailable. FireChat does not, however, replace more private messaging services (Smith, 2014).

VII. Conclusion

The decentralized networks discussed in this paper prove to be unique ways to counter vulnerabilities caused by centralization of traditional Internet structure. However, the success of these networks cannot be judged in contexts beyond countering these vulnerabilities: an application designed to provide connectivity during an Internet shutdown, for example, cannot be proclaimed a failure if it does not protect users from government surveillance. Similarly, programs created to give connectivity and Internet access to underserved communities may seem less successful than a traditional ISP contract when comparing bandwidth capabilities. All of the programs described in this paper, from Commotion in Detroit, to Red Hook's emergency network, to Sudan's crowd-mapping Adena, achieve their developers' goals. While decentralized, community-based networks will likely never fill the same market niche as the ISP-centered Internet, they have great potential to fill other niches, from temporary emergency connectivity to inexpensive, low-bandwidth Internet access. Research should also be pursued that explores the dangerous side of these hard-to-block networks. Just as citizens were able to eschew Iraq's Internet shutdown by using FireChat, a mesh network may provide groups like ISIS, the jihadist rebel group, with the communication capabilities the Iraqi government was trying to thwart. As these decentralized networks develop, then, policymakers, technology-producers, and users must engage in the ever-present discussion of the meaning and importance of freedom of expression and the ability of new technologies to augment, or diminish, the safety of citizens.

References

"About." *Cass Corridor Network Beta*. Accessed November 20, 2014. http://cassco.co/map/about/.

"About Commotion." *Commotion*. Accessed November 20, 2014. https://commotionwireless.net/about.

Abrougui, Afef. "Tunisia: Internet Censorship Makes a Comeback." *Global Voices Online,* May 17, 2011. Accessed November 20, 2014. http://globalvoicesonline.org/2011/05/17/tunisia-internet-censorship-makes-a-comeback/.

"ADVISORY: Detroit Breaking Ground as Lab for Wireless Innovation." *The New America Foundation,* December 18, 2012. Accessed November 20, 2014. http://newamerica.net/pressroom/2012/advisory_detroit_breaking_ground_as_lab_for_wireless_innovation

Anthony, Sebastian. "What is mesh networking, and why Apple's adoption in iOS 7 could change the world." *ExtremeTech,* March 24, 2014. Accessed November 20, 2014. http://www.extremetech.com/computing/179066-what-is-mesh-networking-and-why-apples-adoption-in-ios-7-could-change-the-world.

"AS Rank: Org Ranking." *Center for Applied Internet Data Analysis,* March 2014. Accessed November 20, 2014. http://as-rank.caida.org/?mode0=org-ranking&n=20&ranksort=1.

24, 2014. Accessed November 20, 2014. https://citizenlab.org/2014/07/asia-chats-update-line-kakaotalk-firechat-china/.

Baker, Wayne E. and Kenneth M. Coleman. "Racial segregation and the digital divide in the Detroit metropolitan region." *Edward Elgar,* 2002. Accessed November 20, 2014. http://webuser.bus.umich.edu/wayneb/pdfs/networks/The%20Network%20Society.pdf.

Baraniuk, Chris. "FireChat warns Iraqis that messaging app won't protect privacy." *Wired.co.uk,* June 25, 2014. Accessed November 20, 2014. http://www.wired.co.uk/news/archive/2014-06/25/firechat.

"Beyond the first mile: where your Internet comes from." *OECD Insights,* February 2014. Accessed November 20, 2014. http://oecdinsights.org/2014/02/18/beyond-the-first-mile-where-your-internet-comes-from/.

Brafman, Ori, and Rod A. Beckstrom. *The Starfish and the Spider*. New York: Penguin, 2006.

Brodkin, John. "Democrats grill FCC chairman on Internet fast lanes and ISP mergers." *Ars Technica,* May 20, 2014. Accessed November 20, 2014. http://arstechnica.com/tech-policy/2014/05/democrats-grill-fcc-chairman-on-internet-fast-lanes-and-isp-mergers/.

Brown, Ronald H.. "A Survey of the "Have Nots" in Rural and Urban

America." *The U.S. Department of Commerce,* July 1995. Accessed November 20, 2014. http://www.ntia.doc.gov/ntiahome/fallingthru.html.

Bruno, Raffaele, and Marco Conti. "Mesh Networks: Commodity Multihop Ad Hoc Networks." *IEEE Communications Magazine,* March 2005. Accessed November 20, 2014. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.59.2003&rep=rep1&type=pdf#4.

Byrum, Greta, and Joshua Breitbart. "Wireless organizing in Detroit: Churches as Networked Sites in under-resourced urban areas." *First Monday,* November 4, 2013. Accessed November 20, 2014. http://firstmonday.org/ojs/index.php/fm/article/view/4962/3793.

"Case Study: Mesh Sayada." *The Open Technology Institute,* February 2014. Accessed November 20, 2014. https://commotionwireless.net/files/posts/041814-Case-Study-Sayada.pdf.

"Case Study: Red Hook Initiative WiFi & Tidepools." *The Open Technology Institute,* February 2013. Accessed November 20, 2014. https://commotionwireless.net/files/rhiwifi_tidepools_casestudy.pdf.

Cassidy, John. "We Need Real Competition, Not a Cable-Internet Monopoly." *The New Yorker,* February 13, 2014. Accessed November 20, 2014. http://www.newyorker.com/news/daily-comment/we-need-real-competition-not-a-cable-internet-monopoly.

The Citizen Lab. "Asia Chats: Update on Line, KakaoTalk, and FireChat in China." *University of Toronto,* July

Cohen, Noam. "Hong Kong Protests Propel FireChat Phone-to-Phone App." *The New York Times,* October 5, 2014. Accessed November 20, 2014. http://www.nytimes.com/2014/10/06/technology/hong-kong-protests-propel-a-phone-to-phone-app-.html?_r=2.

Conley, Will. "Ushahidi crowdmapping software reveals silenced Sudanese civil unrest." *Slash Gear,* September 29, 2013. Accessed November 20, 2014. http://www.slashgear.com/ushahidi-crowdmapping-software-reveals-silenced-sudanese-civil-unrest-29299541/.

Cowie, Jim. "Egypt Leaves the Internet." *Dyn Research,* January 27, 2011. Accessed November 20, 2014. http://research.dyn.com/2011/01/egypt-leaves-the-internet/.

Finch, L. "guifi.net, Spain's Wildly Successful DIY Wireless Network." *Rising Voices,* December 11, 2013. Accessed November 20, 2014. http://rising.globalvoicesonline.org/blog/2013/12/11/guifi-net-spains-wildly-successful-diy-wireless-network/.

"FireChat." *iTunes Preview*. November 7, 2014. Accessed November 20, 2014. https://itunes.apple.com/us/app/firechat/id719829352?mt=8.

Gall, Carlotta, and James Glanz. "U.S. Promotes Network to Foil Digital Spying." *The New York Times,* April 20, 2014. Accessed November 20, 2014. http://www.nytimes.com/2014/04/21/us/us-promotes-

network-to-foil-digital-spying.html.
Glans, James, and John Markoff. "Egypt Leaders Found 'Off' Switch for Internet." *The New York Times,* February 15, 2011. Accessed November 20, 2014. http://www.nytimes.com/2011/02/16/technology/16internet.html?_r=2&pagewanted=all&.
Goodman, Jessica. "The Digital Divide Is Still Leaving Americans Behind." *Mashable,* August 18, 2013. Accessed November 20, 2014. http://mashable.com/2013/08/18/digital-divide/.
Gunn, Andy. "Building Community Controlled Digital Infrastructure in Detroit." *The Open Technology Institute,* May 23, 2013. Accessed November 20, 2014. http://oti.newamerica.net/blogposts/2013/building_community_controlled_digital_infrastructure_in_detroit-84570.
Horwitz, Josh. "Unblockable? Unstoppable? FireChat messaging app unites China and Taiwan in free speech… and it's not pretty." *Tech in Asia,* March 31, 2014. Accessed November 20, 2014. https://www.techinasia.com/unblockable-unstoppable-firechat-messaging-app-unites-china-and-taiwan-in-free-speech-and-its-not-pretty/.
"How the Internet refused to abandon Egypt: Authorities take entire country offline... but hackers rally to get the message out." *The Daily Mail,* January 30, 2011. Accessed November 20, 2014. http://www.dailymail.co.uk/news/article-1351904/Egypt-protests-Internet-shut-hackers-message-out.html.
Jensen, Mike. "Promoting the Use of Internet Exchange Points: A Guide to Policy. Management, and Technical Issues."*Internet Society Reports,* 2009. Accessed November 20, 2014. http://www.internetsociety.org/sites/default/files/promote-ixp-guide_0.pdf.
Johnson, Bobbie. "How Egypt Switched off the Internet." *GigaOm,* January 28, 2011. Accessed November 20, 2014. https://gigaom.com/2011/01/28/how-egypt-switched-off-the-internet/.
Kawamoto, Dawn. "Can Google Help Protesters Bypass the Egyptian Internet Shutdown?" *Daily Finance,* February 1, 2011. Accessed November 20, 2014. http://www.dailyfinance.com/2011/02/01/google-twitter-saynow-egypt-protests/.
Kazansky, Becky. "In Red Hook, Mesh Network Connects Sandy Survivors Still Without Power." *Tech President,* November 12, 2012. Accessed November 20, 2014. http://techpresident.com/news/23127/red-hook-mesh-network-connects-sandy-survivors-still-without-power.
King, Jamilah. "A Tech Innovation in Detroit: Connect People, Not Computers." October 3, 2012. Accessed November 20, 2014. http://colorlines.com/archives/2012/10/detroit_mesh_networks.html.

Kuchler, Hannah, and Simeon Kerr. "'Private internet' FireChat app grows in popularity in Iraq." *FT,* June 22, 2014. Accessed November 20, 2014. http://www.ft.com/cms/s/0/ef9602b0-f807-11e3-90fa-00144feabdc0.html#axzz3JzWW6cNT.

Lillah, Sarmad. "Open Garden could be a Revolutionary App, both Technological and Political." *TechFrag,* June 7, 2014. Accessed November 20, 2014. http://techfrag.com/2014/06/07/open-garden-revolutionary-app-technological-political/.

Madory, Doug. "Internet Blackout in Sudan." *Dyn Research,* September 2013. Accessed November 20, 2014. http://research.dyn.com/2013/09/internet-blackout-sudan/.

"Major Media ISP Goes Down." *Buzzfeed,* October 29, 2012. Accessed November 20, 2014. http://buzzfeed.tumblr.com/post/34607165930/major-media-isp-goes-down.

"Member List." *Cairo Internet Exchange*. Accessed November 20, 2014. http://www.caix.net.eg/index.php/member-list.

Meyer, Robinson. "What Firechat's Success in Hong Kong Means for a Global Internet." *The Atlantic,* October 6, 2014. Accessed November 20, 2014. http://www.theatlantic.com/technology/archive/2014/10/firechat-the-hong-kong-protest-tool-aims-to-connect-the-next-billion/381113/.

Oliver, Miquel, Johan Zuidweg, and Michail Batikas. "Wireless Commons against the Digital Divide." *IEEE,* 2010. Accessed November 20, 2014. http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5514608.

"Open Garden." *Crunch Base*. Accessed November 20, 2014. http://www.crunchbase.com/organization/open-garden.

"Our family of apps." *Open Garden*. Accessed November 20, 2014. https://opengarden.com/apps.

"Osona." *Wikipedia*. Accessed November 20, 2014. http://en.wikipedia.org/wiki/Osona.

Ou, Jiayong. "Multipeer Connectivity: A Bag of Hurt." *YMC*, July 15, 2014. Accessed November 20, 2014. http://www.ymc.ch/en/multipeer-connectivity-a-bag-of-hurt.

Paul, Ryan. "The Darknet Project: netroots activists dream of global mesh network." Ars Technica, November 7, 2011. http://arstechnica.com/information-technology/2011/11/the-darknet-plan-netroots-activists-dream-of-global-mesh-network/.

"Percentage of Individuals using the Internet 2000-2012." *International Telecommunications Union (Geneva),* June 2013. Accessed November 20, 2014. http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2013/Individuals_Internet_2000-2012.xls.

Pishevar, Shervin. "Humans Are The Routers." *Tech Crunch,* February 27, 2011. Accessed November 20, 2014. http://techcrunch.com/2011/02/27/humans-are-the-routers/.

Reardon, Marguerite. "Hurricane Sandy disrupts wireless and Internet services." *CNET,* October 30, 2012. Accessed November 20, 2014. http://www.cnet.com/news/hurricane-sandy-disrupts-wireless-and-internet-services/

Rouse, Margaret. "Mesh Network Topology." *TechTarget,* October 2014. Accessed November 20, 2014. http://searchnetworking.techtarget.com/definition/mesh-network.

Simonite, Tom. "Build Your Own Internet with Mobile Mesh Networking." *MIT Technology Review,* July 9, 2013. Accessed November 20, 2014. http://www.technologyreview.com/news/516571/build-your-own-internet-with-mobile-mesh-networking.

Singel, Ryan. "Report: Egypt Shut Down Net With Big Switch, Not Phone Calls." *Wired*.com, February 10, 2011. Accessed November 20, 2014. http://www.wired.com/2011/02/egypt-off-switch/.

Skaar, Ole. "Forget Your ISP: Mesh Networks Are The Future Of The Internet." *Curiosmatic,* February 19, 2014. Accessed November 20, 2014. http://curiousmatic.com/forget-your-isp-mesh-networks-are-the-future-of-the-internet/.

Smith, Matt. "Iraq widens Internet blocks to disrupt insurgent communications." *Reuters,* June 16, 2014. Accessed November 20, 2014. http://www.reuters.com/article/2014/06/16/us-iraq-telecomunications-idUSKBN0ER2WG20140616.

Sperber, Amanda. "Protesters Are Dodging Sudan's Internet Shutdown with a Phone-Powered Crowdmap." *Motherboard,* September 27, 2013. Accessed November 20, 2014. http://motherboard.vice.com/blog/protesters-are-dodging-sudans-internet-shutdown-with-a-phone-powered-crowdmap.

"Tunisia." *Open Net Initiative,* August 7, 2009. Accessed November 20, 2014. https://opennet.net/research/profiles/tunisia.

"What is guifi?" *Guifi.net,* July 6, 2009. Accessed November 20, 2014. http://guifi.net/en/what_is_guifinet.

Vaas, Lisa. "Activists creating decentralized mesh networks that can't be blocked, filtered or silenced." *Naked Security,* February 24, 2012. Accessed November 20, 2014. https://nakedsecurity.sophos.com/2012/02/24/activists-creating-decentralized-mesh-network-that-cant-be-blocked-filtered-or-silenced/.

Valentine, Ben. "Alyx Baldwin: Building Community Through Mesh Networks."[3] *The Civic Beat,* November 16, 2014. Accessed November 20, 2014. http://thecivicbeat.com/2014/11/building-communities-through-mesh-networks/.

[3] On March 25, 2016 the following change was made: JR Baldwin was changed to Alyx Baldwin.