In Defense of The Digital Craftsman:

How Centralized Control of Communications Technologies is Foreclosing 21st Century Craftsmanship

30 June 2015
Submitted: Journal of Peer Production, on the theme: 'Alternative Internets'

Abstract

The increasingly centralized control of communications technologies is foreclosing on the generative potential of the Internet. From commercially-motivated bandwidth throttling and restrictive data caps, to governments blocking websites and services to enforce political or cultural stability, the shift toward command-and-control networking is creating barriers for end-user innovation (Fuchs 2011a; McChesney 2013; Meinrath et al. 2013). Sennett (2008) describes the craftsman (a term which we use here to encompass all genders) as someone with the desire and ability to innovate and adapt a medium and create a new form or function. As networking technologies continue to evolve, the Internet-of-Things affords minimal opportunities for Digital Craftsmanship. In addition to proprietary hardware, control can be engineered throughout networking technologies as well (Galloway 2006; Zittrain 2008); from a technical standpoint, networked technologies are systems of hierarchical layers in which the function of any one layer is interdependent on the other layers of the system (Burns 2003, Van Schewick 2010). Changes in network management protocols and agreed-upon networking standards, locked hardware devices, copyright, patents, digital rights management, and restrictions on data access have the potential to severely limit how end-users can engage with and adapt contemporary networked technologies (Lessig 2002; Meinrath et al. 2011). By contrast, interoperable networks, unlicensed spectrum, open hardware, and access and portability of data provide the foundation for a far more innovative digital ecosystem. By updating prior theorizing (Burns 2003; Benkler 2006; Zittrain 2008), this paper offers a framework for analyzing control of five dimensions of networked technology: networks, devices, applications/services, content, and data. Using this framework, the authors analyze how centralization of control is increasingly hindering innovation, and how open digital platforms offer a far more liberatory alternative that supports future Digital Craftsmanship.

Introducing the Digital Craftsman.

The strength of the Internet, and the foundation for many of the most transformative digital innovations of the last quarter century, has been its openness. Open architectures, open protocols, and open source have supported continuing innovation and disruption; however, contemporary business practices are shifting us away from this historical precedent and instituting ever-increasing centralization of controls over communications technologies that are foreclosing on the potential for Digital Craftsmanship in the 21st century. Tinkering has long been a part of a thriving digital ecosystem -- early hackers turned to computers to improve the complex timing of model trains, while later innovators developed new products in their garages and created hobbyist communities and networked experimentation that drove the transformation of the mainframe computer industry to give rise to the personal computer (Levy 2001). The Internet, an output of an academic-military research project to develop a robust communications network (Curran 2012), pioneered critical changes from previous communications technologies -- as examples, anyone could offer a service over the network, the service could be accessible by anyone on the network, and offering an application or service did not require the permission of network operators (Lessig 2002; Zittrain 2008).

Fundamentally, this permission-free Internet supported the craftsmanship that has defined the innovative ideal of the Internet: the freedom for those with desire and skill to innovate and adapt technologies to create new forms and functions. Unfortunately, while the open and decentralized nature of the Internet has supported this rapid evolution of useful tools, the ever-increasing shift toward command-and-control networking is creating barriers for end-user innovation (Lessig 2002; Zittrain 2008; Meinrath et al. 2013). Changes in network management processes and agreed-upon networking and interconnection standards, locked hardware devices, and acceptable-use restrictions severely limit how end-users can engage with and adapt today's networked technologies (Zittrain 2008; Meinrath et al. 2011).

In 2015, the Internet connects over 8 Billion devices around the world, more than one per person, and Cisco projects that by 2020 there will be 6.5 Internet connected devices for every person on Earth (Evans 2011). The Internet offers an incredible platform for innovation and economic growth (Pélissié du Rausas et al. 2011), but the potential for continuing networked entrepreneurship is under threat. The concept of the "Internet of things", first proposed by Ashton in 1991 (Ashton 2009), has become a conceptual framework that undergirds the regulatory discourse in the United States and Europe, and describes the networking of everyday objects, from computers and thermostats to cars and home appliances (Federal Trade Commission 2013; European Commission n.d.). As this paper illuminates, the mechanisms of control over these networks are creating a relatively locked network of pre-defined, static

objects, rather than a flourishing global digital ecosystem that supports the tinkering, hacking, and new forms of Digital Craftsmanship that will create more liberatory future innovations.

Optimistic scholars have focused on the positive potentials of the growth of the Internet-connected society -- from the new power balances of the information-network mediated society (Castells 2009; Castells 2010), to the support of long-tale markets (Anderson 2008), and the potential of commons-based peer-production afforded by digital networks (Benkler 2006). Other authors have offered more critical perspectives on the detrimental implications of purely capital-driven motivations in the development of networked platforms (McChesney 2013; Fuchs 2011a), and the trend for communications technology to shift from the open tools of tinkerers to the closed technologies of monopoly enclosure (Wu 2011). Key work has also highlighted the regulatory shifts that have supported enclosures of specific aspects of the Internet such as networks (Lessig 2002; Meinrath et al 2011), devices (Lessig 2006, Zittrain 2008) and content (Lessig 2008). Although Benkler (2006), Lessig (2002) and Zittrain (2008) develop a fairly adept technical analysis, Palfrey and Zittrain note that greater understanding of the architecture of technology is needed within the literature (Palfrey and Zittrain 2011) and that previous research does not fully incorporate the implications of the change of locus of control of data from end users to intermediaries.

This paper offers an innovative approach—a technologically-focused analysis of the relationships between the actors and technologies that have created a global "network of networks," and the devices, services, and applications supporting Internet-mediated content and relationships. Rather than focus solely on the role of "Internet of things" technologies, this paper adopts the normative framework that the Internet is a global connector of actors and analyzing the impact of the tensions of five conceptual layers of this global network. Our analysis positions the Internet as mediator of networked relations and focuses on the potential relationship of users to the Internet as an increasingly ubiquitous tool. This framework provides a new methodology for examining how the locus of control supports and/or undermines craftsmanship across five dimensions of networked information and communications technology (ICT): networks, devices, applications/services, content, and data. We document how the lockdown of technologies and centralization of control change the relationships between users and tools, as well as how the limitations to Digital Craftsmanship hamper creativity, lessen the power of the Internet in social movements, undermine the emergence of meaningfully competitive markets, and lead to less liberatory opportunities for Netizens around the globe.

This paper posits "craftsmanship" as a Weberian ideal type of the Internet user (Weber 1947; Cahnman 1976). Although not every user will necessarily offer innovations, and not at all times, the potential for craftsmanship defines the innovative potential of the Internet and offers a framework for understanding the implications of the architecture of networked systems. Sennett argues that craftsmanship emerges from the human desire to do something well, and combined with skill and sufficient control of a medium, drives a user to transform and adapt it (Sennett

2008). Thus, the carpenter reimagining lumber as a chair is one example of a craftsman, as well as the open source developer adapting and improving upon the functionality of a software application (Ibid.); the Digital Craftsman reimagines the functionality and potential of different components of the Internet. Where a potential craftsman may have skill and desire, limited only by their competency with the material in question, with digital technologies, a craftsman's freedom to tinker can be limited by the architecture of the Internet as well as additional digital control planes (Lessig 2002; Zittrain 2008; Meinrath et al. 2011). The perspective of the Digital Craftsman offers an innovative approach in viewing the tensions inherent to digital technologies. Thus, while one perspective of technology studies views the user as a major influencer on the final design of a product (e.g., Bilker 1996), investigating the barriers to craftsmanship offers a renewed focus on the often-subtle enclosures undermining the openness of digital technologies (Winner 1986; Jasanoff 2006; Meinrath et al., 2011).

Reviewing the technological underpinnings and history of the Internet and antecedent communications technologies reinforces how these systems have been designed to limit end-user innovation. As Wu (2011) writes: "History shows a typical progression of information technologies...from a freely accessible channel to one strictly controlled by a single corporation or cartel—from open to closed system" (Wu 2011, p. 6). Wu documents the progression of communications technologies such as radio, telephony, and television, from media that were accessible to tinkerer and innovators, through the regulatory shifts that created barriers to access (e.g., licensure for spectrum, and markets that evolved into monopolies and oligopolies). A closer inspection of the more recent history of the Internet highlights specific dimensions that parallel these prior histories, though often in far more subtle ways.

Telecommunications scholars have often viewed the Internet as a form of commons and a dialectic to investigate constraints and enclosures (Lessig 2002; Benkler 2006; Meinrath et al. 2011). The potential of an Internet commons stems from its open architecture: a standardized, open Internet Protocol that supports the interconnection of networks owned and operated by actors around the globe, with an extensible functionality supporting a diverse array of services and applications ranging from the World Wide Web, email, messaging, media sharing, and games. The Internet's "hour-glass architecture," with a single open protocol interconnecting a diverse array of services and applications which run over a diverse array of media, has traditionally allowed end-users to define how they use the Internet, include sharing their own innovations without permission (Deering 2001; Lessig 2002). The architecture of the Internet, or the code of the technology, is one mechanism for control (Lessig 2008), and a shift towards closed systems and actors leveraging centralized infrastructures have already resulted in new forms of enclosure of this Internet commons (Meinrath et al. 2011).

Zittrain describes systems in terms of generativity in which a third-party or end-user can develop and build upon a device or network (Zittrain 2008). Examples of generative systems include the end-to-end principle of the Internet as well as the rise of the personal computer (which has

traditionally be comprised of a highly extensible platform that interoperates with a huge array of different components). Generativity relies on common standards and flexibilities of the other layers in a system, such as the Internet Protocol and operating system of a computer. Van Schewick describes the alternative as integrated architecture which restrict changing or or modifying other layers (Van Schewick 2010, p. 125).

Digital Craftsmanship offers an expansion on the concept of generativity, one focused on the behavior of the individual in relation to a technology, rather than the technology itself. As the framing of the "Internet of Things" begins to permeate policy discussions, understanding the nuances of the interactions between users and technologies and developing a framework for analyzing networks of human actors encompassing a range of relationships to technology, is critical. The "Digital Craftsman" frame describes an ideal-type relationship: the potential for actors to act with full locus of control over the technologies they use. Digital Craftsmanship assumes that individuals desire to do something well and embodies the potential for entrepreneurial action, the power to innovate, and the freedom to control technologies for their own purposes. However, this relationship is shaped by the tensions between different components of a networked system including the networks, devices, applications/services, content, and data that the Digital Craftsman interacts with. Documenting these components requires understanding both the architectures and control planes of networked systems (Palfrey and Zittrain 2011).

A Five-Layer Analytical Framework.

The politics and tensions of digital technologies such as the Internet can be illustrated by distinguishing amongst the different conceptual dimensions, or layers, of the system. Each layer participates in a hierarchical stack, providing services to the layers above while depending on the layers below (Burns 2003). However, different authors provide different frameworks for analysis of the Internet. For example, one early conceptualization is the Department of Defense (DoD) Model, a four layer model which separates three categories of protocols from physical connections (Burns 2003). The widely-adopted, seven-layer, Open System Interconnection (OSI) model offers a more nuanced stack that focuses on the interoperability and extensibility of the Internet. The seven layers distinguish between three media layers (i.e., physical, data link, and network) and four hosts layers (i.e., transport, session, presentation, and application). In the OSI model the application layer refers to network protocols that facilitate networked services, such as DNS for web browsing, or SMTP and IMAP for email, rather than the services themselves. However, by focusing on the networking elements, these approaches exclude analysis of other components of the system such interconnected devices or the role of digital media platforms.

In order to expand the scope of inquiry beyond to include services supported by digital networks, some scholars have condensed the seven layers of the OSI model into one or two layers and

including additional layers to the top of the stack. Lessig (2002) offers a three-layer model that condenses the OSI model into a physical, code, and content framework. Benkler (2006) similarly uses a three-layer model, with a logical layer providing the functionality of Lessig's code layer. Zittrain (2008) adapts this model, combining the physical and logical (or protocol) layer into a single layer and adding application and social layers. The Application layer represents "the tasks people want might want to perform over the Internet" such as email, viewing video, or messaging (Zittrain 2008, p. 68). These approaches simplify observations of the networking layer while offering a lens to analyze tensions between network routing with physical infrastructure and distribution of content.

This paper offers a five-layered approach building on Zittrain's model. The five technological layers include an undergirding, lowest layer, the technical layer for Zittrain, and the physical layer for Lessig and Benkler, which we call the network layer, in keeping with its function. As well as the introduction of a device layer as the second layer, between the "network" and "application" layers, since unlike traditional computers, contemporary devices (from cell phones to computers to coffee makers) are no longer neutral platforms, but rather control points that interact with and directly shape people's computer mediated experiences.

In addition, above the more traditional application and content layers, we posit that a data layer is crucially important. Security technologist Bruce Schneier characterizes data as "the exhaust of the information age" (Schneier 2015, 17) and can include a user's locations, driving speeds, travel and purchase habits, personal contacts, Internet history, and an ever-increasing array of personal information. As discussed by Losey (2015) this data layer encompasses "the captured information of human interaction with the underlying technology stack" and allows for the analysis of data that is collected, transmitted, and stored as part of end-users' interactions with digital technologies.

These five technical layers support the overarching social layer—activities and interactions facilitated by digital networks—and this model provides a rich framework for analyzing how locus of control over the network, device, application/service, content, and data layers impact the range of interaction with that layer, and amongst and between layers. Although a potential digital craftsman may have the skill and desire to innovate at a given layer, the generativity of a layer may be constrained by actors controlling that given layer or by those below it. The critical characteristic of a layer that supports craftsmanship is a decentralized locus of control at the edges of the networked system that results in end-users and innovators not needing permission for the devices or applications they use, the content they view, or control over their personal data. However, as we document, contemporary technological and legal constraints are instead establishing centralized control and restricting how users can interact with each specific layer. The following section examines several exemplars of this shift in the locus of control across the new five-layer model and analyzes how this centralized control creates barriers undermining innovation by Digital Craftsmen.

Constraining Digital Craftsmanship.

The architecture of a networked technology can support and restrict the level of potential innovation. As Palfrey and Zittrain write: “First, we need to know more about the architecture of the network and how it is changing. For example, is the web becoming more or less centralized over time?” (Palfrey and Zittrain 2011). Using our proposed five-layer approach for analyzing locus of control within the Internet-of-Things ecosystem, this section analyzes several exemplars where Digital Craftsmanship is being detrimentally impacted via centralized control and lock down.

Networks: From Spectrum Scarcity to Data Caps.

The unique architecture of the Internet allows the interconnection of thousands of networks around the world to support a plethora of applications and protocols. The Internet’s architecture demonstrates how a common open Internet Protocol (IP) facilitates the connectivity of numerous networks while supporting a plethora of functions and offering widespread interoperability (Deering 2001; Burns 2003; Zittrain 2008). The Internet’s end-to-end design principle supports applications on the edges of networks rather than through centralized control (Saltzer et al. 1981). Lessig argues that the end-to-end principle of the Internet allows others to provide applications or services without requiring permission of the network operator (Lessig 2002). However, network operators can move away from this standard to limit types of applications, services, or communications.

In April, 2015 Google announced Project Fi, mobile network service that combines Wi-Fi with cellular connectivity on Sprint and T-Mobile networks in the United States (Fox 2015). However, at launch the wireless service is only available using a the Nexus 6, a Google-backed smartphone (Google n.d.). As of this writing, the service is invite-only and Google states that only the Nexus 6 supports a SIM card capable of switching between networks, even though “dual mode phones” are already standard equipment in numerous markets around the globe (Segan 2015). This form of device restriction marks a significant departure from the past half-century of device-flexibility within communications networking.

Prior to the 1968 Carterfone Decision in the United States, telephone subscribers were forbidden from attaching devices to their telephone networks without the express authorization of their telephone provider (Carter et al. v. AT&T et al. 1968). Forbidden devices ranged from the answering machine to plastic privacy-enhancement attachment for handsets called the Hush-A-Phone (Lessig 2002). Without the Carterfone decision, new communications technologies like fax machines and dial-up modems (a core component for user access to the early Internet) would never have come to fruition. But following the Carterfone ruling, wireline Internet users were able to connect the devices of their choosing, and the common Wi-Fi standard extended this

functionality even further. However, today's cellular connections are a far cry from the device-agnosticism of the dial-up Internet. While users should be able to switch SIM cards and join other carrier networks, most phones and tablets are purposefully locked to a single carrier, even though unlocking these devices would cause no meaningful harm to the network. This command-and-control approach to the connection of devices, as history has shown, prevents tinkering and innovation and creates substantial artificial barriers to the introduction of new products.

As the explosion of innovations utilizing unlicensed Wi-Fi exemplifies, access to electromagnetic spectrum allows for for network craftsmanship (De Filippi & Tréguer 2014). Google's Project Fi rents access to Sprint and T-Mobile networks and resells those services while offloading to unlicensed Wi-Fi whenever possible -- providing a potentially game-changing intervention in cellular phone service provision. And in Mexico, indigenous communities underserved by national telecommunications carriers have won access to spectrum to build local low-cost telecommunications networks (The Economist 7 March 2015).

Utilizing two small bands of unlicensed spectrum, at 2.4 GHz and 5.8 GHz, Wi-Fi has not only expanded the reach of Internet access, but also the business models used for broadband service provision as well, from distributed mesh networks for city-wide networks to in-home audio distribution systems. A 2014 study by Telecom Advisory Services estimated that Wi-Fi contributed $222 Billion to the U.S. economy (Katz 2014); however, despite the massive potential of increased unlicensed spectrum, over 95 percent of the public airwaves in the United States (under 30 GHz) are either reserved for governmental use or licensed to private parties, and largely sit unused [1]. Despite the development of spectrum-sharing and cognitive radio technologies, the regulatory approach to spectrum has remained mired in 20th century thinking and the creation of artificial scarcity. Given severely limited access to the public airwaves and the increasing ease of access to software-defined radios, digital craftsmen are likely to become much like copyright infringers who sing Happy Birthday in public -- electromagnetic jaywalkers who are technically breaking the law yet highly unlikely to be prosecuted.

Increasingly, ISPs are implementing data caps on their broadband services -- in essence, limiting how much data a customer can transfer in a given period of time in order to create new pricing tiers based upon customers having to pay for the maximum amount of data they might ever use. Effectively, this represents a shift in billing structure for broadband service from a flat rate to usage based pricing (though users are rarely refunded for using less than their allotment). Data caps present a number of policy challenges that are currently being discussed at the Federal Communications Commision and Federal Trade Commission, and serve as deterrents to broadband adoption, conflicting with federal efforts to increase broadband use. Likewise, data caps directly undermine the shift toward cloud-based (as opposed to local/desktop) computing by creating additional de facto tariffs for data transfers (and potentially resulting in overage charges or even the disconnection of services) (Singel 2011). Additionally, data caps suppress the use of broadband connections for accessing over-the-top video services like Netflix and YouTube (and

any other bandwidth-intensive service or application), presenting a potential barrier to competition that deserves additional scrutiny when Internet Service Providers (ISPs) are already offering their own video content. The use of data caps imposes a false scarcity on data networks and is neither dependent on network costs nor used for reasonable network management, yet the FCC continues to allow this rent-seeking business practice (Brodkin 2015).

At best, data caps serve as a remarkably blunt instrument to reduce overall usage of a network's capacity resources. The use of data caps in Canada serves as a useful case study of the relationship between data caps and congestion. In July, 2010 Canadian ISP Rogers introduced data caps ranging from 2 GB to 175 GB per month (Nowak 2010). Following concerns from users and companies like Netflix, the Canadian Radio-television and Telecommunications Commission (CRTC), which oversees ISP's business practices, began investigating the matter. In July, 2011 Bell executive Mirko Bibic admitted: "No single user or wholesale customer is the cause of congestion" (Lasar 2011), yet at the same time, the reason given to the regulatory authority for the continuance of this business practice was to reduce network congestion.

Caps are an explicit effort to create a scarcity of bytes and impact the types of services customers use via their Internet connections. Minne (2013) argues that data caps on wireline Internet access are intended to ensure that users can "complement, but not replace, traditional subscription TV services," which makes sense when so many ISPs are bundling TV and Internet services. The average American watched nearly 35 hours of television a week (Nielsen 2014). With medium quality stream of Netflix transfers about 700 MB each hour, the average viewer would watch over 100 GB of standard definition video a month; when one looks at high definition (HD) quality content, that usage number can increase by well over 300%.

In 2013 Michael Powell, the former FCC Chairman who went on to become president of the National Cable and Telecommunications Association, acknowledged that the function of data caps was monetization of traffic (Bishop 2013). At the same time, ISPs are entering private arrangements with content providers and applications that would let those services bypass data caps -- a business practice often termed "zero rating" (because use of that service has zero impact on your broadband usage meter). A survey of ISPs globally found 45% of companies offer at least one application that does not incur data charges, and the specifics of these deals differ between ISPs (Morris 2014). In the U.S. AT&T launched a "Sponsored Data" program to allow partners, such as game development companies and advertisers, to offer free content to their customers (AT&T 2014); meanwhile, T-Mobile offers free data for certain music applications (T-Mobile 2014). However, the implications for Digital Craftsmanship is the establishment of a new barrier for new market entrants. Data caps coupled with zero-rating completely undermines network neutrality and end-user control over which content they wish to consume by creating content tiers and complex (hidden) pricing structures. And yet, this growing practice does not, as of the June 2015 FCC rules, run afoul of existing US law, and internationally, this practice is

rapidly growing (although, in 2014, Chile announced that zero-rating would not be allowed; in April 2015, India announced that zero rating would be frowned upon) (Meyer 2014; Wall 2015).

Devices: From Coffee Makers to John Deere Tractors.

The introduction of the personal computer in the 1980s helped make computing more accessible. Pre-packaged, standardized components meant users no longer needed to solder their own boards and created a platform supporting a market for third-party software that could run on these new platforms (Zittrain 2008). And for much of the past 30+ years, PCs have been a neutral medium that would run whatever software they were capable of running and connect to whatever network you plugged them into. However, as the following examples underscore, in recent years, as computational capacity has been built into an array of consumer devices, these new digital ecosystems have become vectors of control rather than interoperability, extensibility, and craftsmanship.

During the 1990s, Green Mountain Coffee Roasters collaborated with Keurig to sell a single-serve pod-based coffee brewing machine, a partnership that facilitated both hardware and coffee pod (k-cup) sales. Green Mountain Coffee Roasters experienced remarkable growth and ended up purchasing Keurig. Meanwhile, the sale of brewers and k-cups went from earning $1.2 Billion in 2010 to $4 Billion by 2014 (McGinn 2013; Dzieza 2015). The popularity of the pod-based brewing system allowed Green Mountain Coffee Roasters to license the pod to other coffee roasters while other coffee companies sold pods independently. However, in 2014 Green Mountain Coffee Roasters, renamed Keurig Green Mountain, integrated Digital Rights Management (DRM) into the 2.0 version of their k-cups. These new machines included a infra-red scanner that would detect special ink markings on Keurig coffee pods and would cause the machine to fail to work if users attempted to brew unlicensed coffee pods in these "new-and-improved" Keurig machines (Dzieza 2014). The release of DRM coffee proved to be a poor business decision, in part because Keurig 2.0 machines not only locked out competitors coffee pods, but also Keurig's own 1.0 pods (and the Keurig refillable pod), resulting in a steep decline in sales (Dzieza 2015). In May 2015, following a ten-percent decline in share price Keurig acknowledged the error in forcing consumers to purchase single-use pods and announced a plan to brew unlicensed coffee brands (Geuss 2015). However, their change of heart was laced with language that would seem to undermine the initial "win" (Barrett 2015) -- Keurig is not planning to remove the DRM, but rather, to make licensing of DRM-equipped k-cups more widespread (Kline 2015). Ensuring that your choice of coffee will be prescribed, not solely by your own proclivities, but mediated through the licensure practices of the manufacturer of our coffee maker.

Keurig's incorporation of DRM demonstrates how legal and technical concepts first introduced as copyright protection measures are built into computing devices to control the sale of add-on services or products. For example, new tractors, such as those from John Deere, lock end-users

out of making repairs or modifications via both technical limitations and end-user acceptable use policies. Likewise, more and more new cars have Electronic Control Units (ECUs) that prescribe everything from powertrain operations to the battery management. Access to the ECU software is required both for diagnosing the computer for repair as well as modifying the car for better gas milage. However, these types of modifications—the digital equivalents of tinkering on your own car—are illegal on many of these vehicles.

In 1998, the U.S. introduced the Digital Millennium Copyright Act (DMCA), which criminalizes circumventing digital rights management, regardless of the intention of this circumvention (Lessig 2002). When applied to consumer goods, this effectively redefines ownership of everything from vehicles and coffee machines (i.e., just because you own that device, no longer grants you the right to do with it as you please). As Benkler writes, the result is that the DMCA favors "giving the copyright owner a power to extinguish the user's privileged uses" (Benkler 1999, p. 421). Although the US Copyright Office conducts a triennial review of DMCA exemptions, companies actively defend their locked-down products, and in doing so, insist consumers do not fully own what they have purchased (Bartholomew 2015; Lightsey & Fitzgerald 2015). John Deere defends their own practices by arguing that consumers who purchase their tractors "cannot properly be considered the 'owner' of the vehicle software" (Bartholomew 2015). General Motors also states that end-users merely license the software running their car (Lightsey & Fitzgerald 2015). While the traditional mechanical craftsman could repair their own tractor the 21st century digital craftsman is prevented by law from doing so.

Applications: WWW vs. Facebook.

In 1990 Tim Berners-Lee began distributing his innovation of linking pages of content over shared computer networks. His innovations, including hypertext transport protocol (HTTP), became the foundation for the World Wide Web. Offered without patent or fee for use, HTTP and HTML allowed digital craftsmen to develop webpages for news, video sharing, search, and social media. The Web became the "killer application" for the Internet—the essential application that drove mainstream adoption. However, as with any powerful tool, liberatory potential of any application is often mirrored by an equally oppressive potential trajectory. While Mosaic and later graphical web browsers like Netscape, Internet Explorer, Firefox and Chrome make the Web accessible over the open Internet, applications can also constrain the user experience in both obvious and subtle ways. which networked sites are available.

In 2010, FaceBook launched Facebook Zero, a text-only zero-rated version used by partnering telecom carriers. Over the next three years, ten-percent of Facebook's billion+ active users used FaceBook Zero (Russell 2013). In August, 2013 Facebook launched Internet.org, a zero-rated application whose initial goal was "to make Internet access available to the two-thirds of the world who are not yet connected, and to bring the same opportunities to everyone that the connected third of the world has today" (Facebook 2013). Internet.org was partnership with

Facebook, Ericsson, MediaTek, Nokia, Opera, Qualcomm and Samsung and first rolled out with Airtel in Zambi in 2014 (Cooper 2014).

However, the Internet.org app is very different that the Internet and the Web. While the World Wide Web offers an range of accessible information limited only by the pages end users create, the Internet.org application offers a limited range of pages and applications. At launch in Zambia these included AccuWeather, Go Zambia Jobs, Wikipedia, and Facebook. These pages offer services to users, but as a limited set, they more resemble channels on cable television rather than a democratic communications platform. Furthermore, this limited set of services is not the Web, and fails to provide the same generative potential that Zittrain ascribes to the Web (Zittrain 2008). Internet.org is an application-based portal to information channels, an Internet experience mediated by a corporate consortium rather than end users themselves. This is the obvious difference, but it is also the case that Facebook on Facebook Zero is actually different than the Facebook people experience when they access the platform over normal Internet connections. Unbeknownst to most people, Facebook Zero's Facebook is actually stripped of much of its rich content (e.g., pictures, videos) -- making for a resource-poor variant that, by Facebook's own estimate, is passed off to hundreds of millions of the world's poor as "separate, but equal."

In May 2015, Mark Zuckerberg, co-founder of Facebook and Internet.org, announced the launch of the Internet.org platform through which developers could offer pages or services via a zero-rating Facebook Zero platform. Opening Internet.org is widely seen as positive step to providing more connectivity to users; however, channelling the "Internet" experiences of the world's poor through a gatekeeper application is not a good option for expanding Digital Craftsmanship, so much as a bait-and-switch business practice that will eventually leave billions on the wrong side of a new, subtle, but very real, digital divide.

Not all countries have given Internet.org a positive reception. Facebook launched Internet.org in India in February 2015 through a partnership with Reliance Communications (Facebook 2015). At launch, the service provided access to 38 websites and services in six Indian states. Following this rollout, Kiran Jonnalagadda, founder of HasGeek, a hacker convening in Bangalore, India, helped launch a campaign to oppose Internet.org in India. The #SaveTheInternet campaign directed participants to email the Telecom Regulatory Authority of India (TRAI) regarding their questionnaire "Regulatory Framework for Over-the-top (OTT) services / Internet services and Net Neutrality." In response to the growing public outcry, in April 2015, Indian companies began pulling out of Internet.org, even though TRAI had not officially ruled if zero-rating and Internet.org would be perimited (Wall 2015).

Content: Remixes and Political Speech.

Networked technologies have supported new paradigms of information dissemination, including what Castells describes as mass-self communication, and the growth of independent content producers (Castells 2010). The role of individual content production has been described as an important shift in collective action and contentious political debate (Bimber et al. 2012; Bennett & Segerberg 2013; Milan 2015). At the same time, copyright enforcement mechanisms and the inclusion of copyright maximalist goals in trade agreements has further centralized surveillance over and control of content.

Remixing and Networked Advocacy

In January 2012, a Germany-based Anonymous cell uploaded the video "Was ist ACTA?" highlighting Internet censorships and increased copyright restrictions contained in leaked Anti-Counterfeiting Trade Agreement (ACTA) texts (Anonymous Germany 2012). The video, the most popular anti-ACTA video to date, is a remix—an adaptation of a previously released original video. The creators of "Was ist ACTA" redubbed a 2010 English video from a Hamburg-based Anonymous cell that in turn animated and expanded on published ACTA analysis from the Paris-based organization La Quadrature du Net (liekmudkip 2010; Losey 2014). The German-language video proved essential to organizing opposition to ACTA, proliferating on German game forums and receiving over 1 million viewers. Anti-ACTA organizers cited the video's reach as an important contributor to streets protests against the Agreement (Losey 2013).

Remixing videos well predates the Internet, and artists certainly also created and shared videos in the pre-YouTube era. For example, Swedish remix artist Johan Söderberg started his "Read My Lips" series of videos editing clips of world leaders to look like they are singing pop songs as a form of political critique beginning in 2001 (McIntosh 2012). And the popular satirical news program *The Daily Show* frequently uses reappropriation of news commentary and statements.

The extent that the Internet can support individual cultural production has been important component of digitally-mediated political action for years, both through individual action and as an organizing construct. The "We are the 99%" meme helped grow Occupy Wall Street protests in New York and globally. Bennett and Segerberg describe how the Occupy meme "quickly traveled the world via personal stories and images shared on social networks such as Tumblr, Twitter, and Facebook" (Bennett and Segerberg 2013, loc. 742). Ganesh and Stohl (2013) documented how the Occupy frame inspired complimentary protests as far away as Wellington, New Zealand. Wolfson (2014) describes how a commitment to open-content publishing and journalism created the foundation of the Indymedia movement, which was the first global foray into citizen journalism that utilized both new digital media production technologies and the Internet as a content-distribution system and open publishing platform.

Copyright vs. Open Publishing.

Copyright regimes are used and abused to restrict content. The DMCA, which John Deere and GM are using to restrict even the most basic device-level craftsmanship on their vehicles, actively restricts access to key diagnostic software and even includes a framework for removing content from websites. Under the DMCA, US-based websites can be held liable for hosting copyrighted material if the offending material is not removed after receiving an infringement claim, and most online forums abide by these take-down notices, even when they are clearly bogus (for example, Tumblr's recent compliance with a DCMA takedown notice from a man who claims to be channeling an alien from the future that has copyright over other artists' digital works) (Geigner 2015).

Although notice-and-takedown regimes and decreased intermediary liability and supports greater freedom of expression, the DMCA is most often used by automated "take-down notice mills" that are creating millions of notices with next to zero checks and balance for fair use (and often are complied with with no actual human review). As Seltzer writes "The DMCA safe harbors may help the service provider and the copyright claimant, but they hurt the parties who were absent from the copyright bargaining table" (Seltzer 2010, p. 177). And this doesn't just impact "the little guys." During the 2008 U.S. Presidential elections, Republican nominee Senator John McCain had videos removed from YouTube, including content from newscasts that were removed after YouTube received DMCA from news organizations (Sohn & McDiarmid 2010). In April, 2015 U.S. Senator Rand Paul announced his candidacy for the Republican presidential nomination in the United States. His announcement video was automatically removed by YouTube's copyright Content ID system because video included clips from John Rich's 2009 song Shuttin' Detroit Down (Bump 2015). And even Lawrence Lessig has had YouTube videos of his lectures on fair use removed via take-down notices wrongfully claiming copyright infringement (Andy 2014).

The DMCA has been abused in efforts to silence critique. Benkler describes how ATM and election machine manufacturer Diebold forced students at Swarthmore University to remove emails that documented the company's internal concerns over the security of their voting machines (Benkler 2006). A decade later, in 2015 News Corp. sent a DMCA request to First Look media including an image of the front page of the Sunday Times in a critique of an article published on the page (Mullin 2015). By contrast, Anonymous Hamburg shared their 2010 ACTA video under a Creative Commons license specifically to avoid DMCA takedowns of later adaptations or mirrors. Creative Commons is a licensing framework that allows content creators to choose to retain some rights while granting permissionless rights to others, such as reuse or remixing. The license ensured the legality of mirror uploads and the 2012 German translation, but does not guarantee longevity of later uploads. For example, in 2012 NASA uploaded their video of the Mars Rover landing on Mars. NASA's video is public domain and was also used by commercial news services, one of which issued a DMCA takedown request on NASA's original

upload (Pasternack 2012). Indeed, law professor and Creative Commons co-founder Lessig acknowledges the licensing system is "a step to rational copyright reform, not itself an ultimate solution" (Lessig 2008, p. 279).

Cultural production, including remixing, is a craft requiring technical skill. From fandom such as Anime Music Videos (Knobel and Lankshear 2008; Ito 2010) to political appropriation (McIntosh 2012) and participation in memes (Castells 2012; Bennett and Segerberg 2013), content production allows individuals to participate in shared communities and cultural dialog. Developing digital literacy to participate in community offers educational opportunities (Knobel and Lankshear 2008), while copyright regimes that overstep the bounds and often utterly ignore fair use to maximize profits create unnecessary (and often illegal) restrictions to digital craftsmanship and stifle freedom of expression.

Data: Creation and Control.

With the growth of the Internet-of-Things, networked data collection is rapidly moving beyond web browsing habits to include a far more panoptic range of devices, from wearable fitness trackers like Fitbit, to refrigerators, and vehicles. Today, farmers are beginning to use GPS mixed with local field data to automate their tractors (Lowenberg-DeBoer 2015), and these data are, in turn being collected by the manufacturers of these tractors for unknown purposes. While collecting and utilizing these data can create new economic opportunities and open doors for new innovations, with the locus of control over these data often well outside the hands of the users of these devices and services, these tools are often used to commercialize, rather than empower, digital craftsmen.

In June 2015, fitness tracker device company Fitbit had their initial public offering at $20 USD per share. Through its wearable fitness device, Fitbit sells the consumer a service: the ability to track data about one's movements and activities. This service is quite valuable, and current Fitbit dominates with 85% of the market -- by the closing bell on its first day of trading, Fitbit's shares had increased 50%, achieving a $6 Billion market capitalization on its first day of trading (Driebusch 2015). Clearly, data collection, processing, and sales have created significant economic opportunities, and incentives for control.

In 2013, Jeff Leak, an assistant professor in biostatistics at John Hopkins University, began experimenting with his Fitbit data. He quickly realized that although his Fitbit collects minute-by-minute data, access to these data was limited to Fitbit Partners (Leek 2013). Access to this stream is negotiated through third-party apps with access agreements with Fitbit. Although some digital craftsman have found that they have been able to request personal access by email Fitbit (Ramirez 2014), controlling access to data streams is often a difficult proposition. Usually, data collected by Internet-of-Things devices is managed through a command-and-control model that extracts personal information and stores them in central repositories controlled by the

service/device/applications provider, not the user. While some form of (usually read-only) access is often made available through APIs, this access is almost always severely limited and changes over time. For example, in 2012, Twitter introduced new restrictions on how much data third-party applications could access (Kern 2012). In doing so, Twitter blocked third-party interfaces, and pushed users to use the official Twitter mobile app, rather than the growing host of more diverse access applications. Likewise, researchers analyzing Twitter data were locked out of this proprietary data store as well.

The value open data in the EU27 was estimated in excess of $40 Billion in 2010, and has grown substantially since then (Tinholt 2013). Globally, McKinsey estimates that data, in open sharable formats, can generate $3-5 trillion in economic growth. However, emerging end-user computing devices not only have limited data-access interfaces, but the data they collect is increasingly tethered to the device and central storage systems and often considered proprietary.

End-user access to data allows individual entrepreneurship, for example, using granular energy use information to maximize the efficiency of electrical use or driving habits -- which, as Nest, a connected thermostat offered from Google, exemplifies, is a growing business model (Olson 2014). This ability for users to access and utilize our own data allows digital craftsmen to develop and share tools that are built on top of this data layer. Additional applications can then combine data sets, for example, from smart meters, in-home appliances and control interfaces, to better match usage to budgets and interests. End-user applications could also encrypt and locally store data to increase user privacy, a solution to the growing problem of centralized data stores being regularly hacked due to inadequate operational security precautions.

LastPass is a networked password manager. Rather than remember dozens of passwords for applications, files, and logins across devices, LastPass allows users to login using a master password. However, because the service centrally stores these passwords LastPass is a honeypot -- a desirable target for hackers around the globe. In June 2015, LastPass announced that they had been hacked, and although master passwords are encrypted on user devices locally before being transmitted to a central server, hashes from these passwords were accessed, requiring users to change their passwords (Siegrist 2015). Hacks of central data stores are a substantial and growing risk of the Internet-of-Things. For example, in 2014, Apple's iCloud service was hacked, leading to the release of nude personal photos of dozens of celebrities; and, in 2012, a Facebook bug enabled some accounts to be accessed without a password.

Computer security expert, Bruce Schneier, frames the relationship between users and tech companies as "Feudal Security," a concept that builds upon the Meinrath et al.'s theory of digital feudalism (Meinrath et al. 2011). Feudal Security highlights the dependency of end-users on the companies that collect, transmit, and store their data (Schneier 2012). Schneier acknowledges that while Feudal Security reduces the cost of technological individual expertise in exchange for

implicit corporate trust, at the same time, corporate-only solutions prevent individuals from taking control over their own data (Schneier 2013).

The political economy of the Internet incentivizes the collection of end-user data (Fuchs 2011b), and companies collaborate willingingly and unwillingly with large-scale law enforcement surveillance (Meinrath & Vitka 2014). After the revelations of the Edward Snowden leaks, the specter of government surveillance that permeates phone calls, emails, and stored data has become increasingly alarming. The economic fallout includes a German company building a $1.2 Billion data center to avoid using US cloud services, and total losses to the U.S. tech industry could reach 25% of the total industry's market share (Miller 2014). At the same time, surveillance is generating a demand for new, user-friendly secure communications tools. However, the ability to develop tools that secure the data layer require end-user control of data transmission and cooperation—ideally permission-free access—of underlying layers. Enclosing the data created from the Internet-of-Things in corporate-controlled digital ecosystems severely limits the ability of digital craftsmen to develop meaningfully secure protections over their personal data.

The Future of Digital Craftsmanship.

Over the next decade, the number of networked devices is expected to grow by an order of magnitude; however, the locus of control over networks, devices, applications, content, and data will determine the extent that Digital Craftsmanship will continue to thrive. If the agility and independence of any one of these layers is subsumed by dominant market players within any other layer, the economic value of that incorporated layer will be decreased and future innovative potential will be dramatically curtailed. A future that protects end-user innovation must take this into account, especially as we enter an Internet-of-Things era. This includes the ability to use and innovate without the permission of the network (Lessig 2002), as well as preventing one layer from foreclosing on the generativity of another (Zittrain 2008). The extent that corporate control is allowed to encroach upon the potential for Digital Craftsmanship will determine the parameters of "ownership" in the 21st century.

This paper provides a conceptual model for understanding the Internet-of-Things as a network of mediated relationships in which the architectures and controls over the corresponding layers of networked systems directly impact the range of freedom of users' experiences. Each layer offers distinct potentials for innovation and concomitant risks via centralized control. Although historically, the Internet has been as a platform for permissionless innovation, this paper documents the increasing array of business practices that are actively undermining Digital Craftsmanship.

Entrepreneurs, policy makers, and careful and critical observers must look beyond the surface-

level technologies of networked systems and interrogate the technological underpinnings to contemporary and future digital technologies (as well as their positive and negative repercussions). We provide a parsimonious framework for understanding how the politics within and between technological layers of networked systems change the relationship between users and technologies. This framework focuses on the relationship between users and the networked communications tools we seek to utilize. The future of Digital Craftsmanship will pit the liberatory potential of these new technologies against corporate forces seeking to create feudalistic digital ecosystems, with the outcome determining whether we have the ability to innovate and tinker, or whether we become digital serfs facing an ever-more-oppressive panoptic and extractive networked world.

End Note

[1] In cases like the citizens' band (CB) spectrum is set aside for amateur use, or according to "Part 15" rules which allow some public wireless devices such as garage door openers and microwave ovens to operate in unlicensed spectrum. See Bennett Z. Kobb, Wireless Spectrum Finder: Telecommunications, Government and Scientific Radio Frequency Allocations in the US 30 MHz - 300 GHz (McGraw-Hill 2001), and National Telecommunications and Information Administration, Manual of Regulations and Procedures for Federal Radio Frequency Management (Redbook), (Washington: US Government Printing Office, 2008).

References

Anderson, C 2008, *The Long Tail: Why the Future of Business is Selling Less of More*, Revised Edition, Hachette Books, New York.

Andy 2014, "Tumblr Complies With DMCA Takedown Requests From A Self-Proclaimed Future-Alien From Another Planet", *Torrent Freak* 23 June. Available from: https://www.techdirt.com/articles/20150618/14264131389/tumblr-complies-with-dmca-takedown-requests-self-proclaimed-future-alien-another-planet.shtml [30 June 2015].

Anonymous Germany 2012, Anonymous - Was ist ACTA? - #StopACTA [german sync], (video file), Available from: https://www.youtube.com/watch?v=9LEhf7pP3Pw [30 June 2015].

Ashton, K 2009, "That 'Internet of Things' Thing", *RFiD Journal 22*, no. 7, pp. 97-114.

AT&T 2014, AT&T Introduces Sponsored Data for Mobile Data Subscribers and Businesses, 6 January 2014. Available from: http://www.att.com/gen/press-room?pid=25183&cdvn=news&newsarticleid=37366&mapcode= [30 June 2015].

Barrett, B 2015, "Keurig's My K-Cup Retreat Shows We Can Beat DRM", *Wired* 8 May. Available from: http://www.wired.com/2015/05/keurig-k-cup-drm/ [30 June 2015].

Batholomew, D 2015, Long Comment Regarding a Proposed Exemption Under 17 U.S.C. 1201 United States Copyright Office, Library of Congress, Docket No. 2014-07 Proposed Class 21: Vehicle Software – Diagnosis, Repair, or Modification. Available from: http://copyright.gov/1201/2015/comments-032715/class%2021/John_Deere_Class21_1201_2014.pdf [30 June 2015].

Benkler, Yochai. "Free as the Air to Common use: First Amendment Constraints on Enclosure of the Public Domain", NYU Law Rev. 74 (1999): 354.

Benkler, Y. 2006, *Wealth of Networks: How Social Production Transforms Markets and Freedom*. Yale University Press, New Haven.

Bennett, WL, & Segerberg, A 2013, *The Logic of Connective Action: Digital Media and the Personalization of Contentious Politics*. Cambridge University Press, New York.

Bijker, Wiebe E 1996 *On Bikes, Bakelite and Bulbs: Towards a Theory of Socio-Technical Change*. MIT University Press, Cambridge.

Bimber, BA, Flanagin AJ & Stohl, C 2012, *Collective Action in Organizations: Interaction and Engagement in an Era of Technological Change*, Cambridge University Press, New York.

Bishop, B 2013, "Former FCC Chairman admits data caps aren't about preventing network congestion", *The Verge* 18 January. Available from: http://www.theverge.com/2013/1/18/3892410/former-fcc-chairman-admits-data-caps-arent-about-preventing-network-congestion [30 June 2015].

Brodkin, J 2015, "AT&T still throttles unlimited data, and FCC isn't promising to stop it", *Ars Technica* 12 March. Available from: http://arstechnica.com/business/2015/03/att-still-throttles-unlimited-data-and-fcc-isnt-promising-to-stop-it/ [30 June 2015].

Bump, P 2015, "YouTube's copyright system has taken Rand Paul's presidential announcement offline", *The Washington Post* 7 April. Available from: http://www.washingtonpost.com/blogs/the-fix/wp/2015/04/07/youtubes-copyright-system-has-taken-rand-pauls-presidential-announcement-offline/ [30 June 2015].

Burns, K 2003, *Tcp/Ip Analysis & Troubleshooting Toolki*t, John Wiley & Sons.

Cahnman, WJ 1965, "Ideal Type Theory: Max Weber's Concept and Some of Its Derivations", *The Sociological Quarterly* vol. 6, no. 3 pp. 268-280.

Castells, M 2009, *Communications Power*, Oxford University Press, Oxford.

Castells, M 2009. *The Rise of the Network Society Vol. 1*, Blackwell Publishers, Oxford. Second Edition.

Castells, M 2012, *Networks of Outrage and Hope*, Polity Press, Cambridge.

Coleman, EG 2013, *Coding freedom: The Ethics and Aesthetics of Hacking*, Princeton University Press, Princeton.

Cooper, P 2014, "Facebook finally rolls out Internet.org, bringing free Internet to Africa", *IT Pro Portal* 31 July. Available from: http://www.itproportal.com/2014/07/31/facebook-finally-rolls-out-internetorg-bringing-free-internet-to-africa [30 June 2015].

Curran, J 2012,"Rethinking Internet History" in *Misunderstanding the Internet,* eds J Curran, N Fenton & D Freedman, Routledge, London, pp. 34-65.

De Filippi, P &, and Tréguer, F, 2014 “Expanding the Internet Commons: The Subversive Potential of Wireless Community Networks”, *Journal of Peer Production*, no. 6, pp 1-11.

Deering, S 2001, “Watching the Waist of the Protocol Hourglass”, *IETF* no. 51, London, August,. Available from http://www.iab.org/wp-content/IAB-uploads/2011/03/hourglass-london-ietf.pdf [30 June 2015].

Driebusch, C 2015, “Fitbit IPO Prices at $20 a Share, Above Expectations”, *The Wall Street Journal* 17 June. Available from: http://www.wsj.com/articles/fitbit-ipo-prices-at-20-a-share-above-expectations-1434582147 [30 June 2015].

Dzieza, J 2014, “Inside Keurig's plan to stop you from buying knockoff K-Cups”, *The Verge* 30 June. Available from: http://www.theverge.com/2014/6/30/5857030/keurig-digital-rights-management-coffee-pod-pirates [30 June 2015].

Dzieza, J 2015, “Keurig's attempt to 'DRM' its coffee cups totally backfired”, *The Verge* 5 February. Available from: http://www.theverge.com/2015/2/5/7986327/keurigs-attempt-to-drm-its-coffee-cups-totally-backfired [30 June 2015].

Edwards, R, & Tryon, C 2009, “Political Video Mashups as Allegories of Citizen Empowerment”, *First Monday*, vol. 14, no. 10.

The Digital Millennium Copyright Act, 1998, Pub. L. No. 105–304, 112 Stat. 2860, October 28, Available from www.copyright.gov/legislation/dmca.pdf. [30 June 2015]

The Economist 2015, “DIY Telecoms”, *The Economist* 7 March. Available from: http://www.economist.com/news/technology-quarterly/21645498-fed-up-failings-big-operators-remote-mexican-communities-are-acting 30 june 2015.

European Commission n.d., “The Internet of Things”, *Digital Agenda For Europe*. Available from: http://ec.europa.eu/digital-agenda/en/internet-things [30 June 2015].

Evans, D 2011, “The Internet of Things: How the Next Evolution of the Internet is Changing Everything”, *CISCO White Paper*. Available from: http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf [30 June 2015].

Facebook 2013, Technology Leaders Launch Partnership to Make Internet Access Available to All, *Press Release* 21 August 2013. Available from: https://newsroom.fb.com/news/2013/08/technology-leaders-launch-partnership-to-make-internet-access-available-to-all/ [30 June 2015].

Facebook 2015, Internet.org App Now Available in India, *Press Release* 10 February 2015. Available from: http://newsroom.fb.com/news/2015/02/internet-org-app-now-available-in-india/ [30 June 2015].

Federal Trade Commission 2015, "Internet of Things—Privacy and Security in a Connected World". Available from: https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf [30 June 2015].

Fox, N 2015, Say hi to Fi: A new way to say hello, 22 April 2015, Google Official Blog. Available from: http://googleblog.blogspot.se/2015/04/project-fi.html [30 June 2015].

Fuchs, C 2011a. *Foundations of Critical Media and Information Studies*, Taylor & Francis.

Fuchs, C 2011b, "New Media, Web 2.0 and Surveillance", *Sociology Compass, vol.* 5, no. 2 pp.134-147.

Ganesh, S, & Stohl, C. 2013, "From Wall Street to Wellington: Protests in an era of digital ubiquity", *Communication Monographs* vol. 80, no. 4, pp. 425-451.

Geuss, M 2015, "Keurig says it was wrong to force users to buy single-serving pods", *Ars Technica* 7 May. Available from: http://arstechnica.com/business/2015/05/keurig-stock-drops-10-percent-says-it-was-wrong-about-drm-coffee-pods/ [30 June 2015].

Geigner, T 2015, "Tumblr Complies With DMCA Takedown Requests From A Self-Proclaimed Future-Alien From Another Planet", *Techdirt* 23 June. Available from: https://www.techdirt.com/articles/20150618/14264131389/tumblr-complies-with-dmca-takedown-requests-self-proclaimed-future-alien-another-planet.shtml [30 June 2015].

Google n.d., Network. Available from: https://fi.google.com/about/network/ [30 June 2015].

Howard, PN 2015. *Pax Technica: How the Internet of Things May Set Us Free or Lock Us Up*, Yale University Press: New Haven.

Ito, M 2010, "The rewards of non-commercial production: Distinctions and Status in the Anime Music Video Scene", *First Monday, vol.* 15, no. 5.

Jasanoff, S 2006, "Technology as a Site and Object of Politics" in *The Oxford Handbook of Contextual Political Analysis* eds. RE Goodin & C Tilly, Oxford University Press, Oxford, pp. 745-763.

Katz, R 2014, Assessment of the Economic Value of Unlicensed Spectrum in the United States, Telecom Advisory Services, LLC, Report, February. Available from: http://www.wififorward.org/wp-content/uploads/2014/01/Value-of-Unlicensed-Spectrum-to-the-US-Economy-Full-Report.pdf [30 June 2015].

Kern, E 2012, "Game changer: Twitter rolls out expected restrictions to API use", *GigaOm 16 August.* Available from: https://gigaom.com/2012/08/16/twitter-rolls-out-expected-restrictions-to-api-use/ [30 June 2015].

Kline, DB 2015, "What Keurig's New Stance On DRM Means for Unlicensed K-Cups", *Motley Fool* 11 May. Available from: http://www.fool.com/investing/general/2015/05/11/what-keurigs-new-stance-on-drm-means-for-unlicense.aspx [30 June 2015].

Knobel, M & Lankshear C 2008, "Remix: The Art and Craft of Endless Hybridization", *Journal of Adolescent & Adult Literacy, vol.* 52, no. 1 pp. 22-33.

Lasar, M 2011, "Metered billing: it's a lack of competition, not congestion", *Ars Technica* 12 July. Available from: http://arstechnica.com/tech-policy/2011/07/metered-billing-its-a-lack-of-competition-not-congestion/ [30 June 2015].

Leek, J 2013, Fitbit, why can't I have my data?. 2 January 2013. *Jeff Leek: Blog.* Available from: http://simplystatistics.org/2013/01/02/fitbit-why-cant-i-have-my-data/ [30 June 2015].

Lessig, L 2002, *The Future of Ideas: the Fate of the Commons in a Connected World*, Vintage Books, London.

Lessig, L 2006, *Code Version 2.0*. Basic Books, New York.

Lessig, L 2008, *Remix: Making Art and Culture Thrive in the Hybrid Economy*, Penguin Books, New York.

Levy, S, 2001, *Hackers: Heroes of the Computer Revolution*, Penguin Books, New York.

liekmudkip 2010, NO ACTA - Stop the Krake, (video file), Available from: https://www.youtube.com/watch?v=qlFyoEKV0dE [30 June 2015].

Lightsey, HM & Fitzgerald, AQ 2015, Comments of General Motors LLC, United States Copyright Office, Library of Congress, Docket No. 2014-07 Proposed Class 21: Vehicle Software – Diagnosis, Repair, or Modification. Available from: http://copyright.gov/1201/2015/comments-032715/class%2021/General_Motors_Class21_1201_2014.pdf [30 June 2015].

Losey, J 2014, "The Anti-Counterfeiting Trade Agreement and European Civil Society: A Case Study on Networked Advocacy", *Journal of Information Policy vol.* 4, pp. 205-227.

Losey, J 2015, "The Locus of Control in Networked Communications: Implications for Collective Action", Paper presented at *International Communications Association Annual Conference: Communications Across the Lifespan*.

Lowenberg-DeBoer, J 2015, "The Precision Agriculture Revolution", *Foreign Affairs vol.* 94, no. 3, pp. 105-112.

Manyika, J, Chui, M, Farrell, D, Van Kuiken, S. Groves, P, & Doshi, EA 2014, "Open Data: Unlocking Innovation and Performance With Liquid Information" McKinsey & Company. Available from: http://www.mckinsey.com/insights/business_technology/open_data_unlocking_innovation_and_performance_with_liquid_information [30 June 2015].

McChesney, RW 2013, *Digital Disconnect: How Capitalism is Turning the Internet Against Democracy*, The New Press, New York.

McGinn, D 2011, "The Buzz Machine", *The Boston Globe* 7 August. Available from: http://www.boston.com/business/articles/2011/08/07/the_inside_story_of_keurigs_rise_to_a_billion_dollar_coffee_empire/?page=6 [30 June 2015].

McIntosh, J 2012, "A History of Subversive Remix Video before YouTube: Thirty Political Video Mashups Made between World War II and 2005", *Transformative Works and Cultures*, no. 9.

Meinrath, SD, Losey, J & Pickard, VW 2001, "Digital Feudalism: Enclosures and Erasures from the Digital Rights Management to the Digital Divide", *Commlaw Conspectus*, vol. 19, pp.423–479.

Meinrath, SD & Vitka, S 2014, "Crypto War II", *Critical Studies in Media Communication*, vol. 31, no. 2, pp. 123-128.

Meyer, D 2014, "In Chile, mobile carriers can no longer offer free Twitter, Facebook or WhatsApp", *GigaOm* 28 May. Available from: https://gigaom.com/2014/05/28/in-chile-mobile-carriers-can-no-longer-offer-free-twitter-facebook-and-whatsapp/ [30 June 2015].

Milan, S 2015, "From Social movements to Cloud Protesting: The Evolution of Collective Identity", *Information, Communication & Society* vol 0, no. 0, pp. 1–14.

Miller, CC 2014 “Revelations of N.S.A. Spying Cost U.S. Tech Companies”, *The New York Times* 21 March. Available from: http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html [30 June 2015].

Minne, J 2013, “Data Caps: How ISPs are Stunting the Growth of Online Video Distributors and What Regulators Can Do About It”, *Fed. Comm. LJ*, vol. 65 pp. 234-260.

Morris, A 2014, “Report: 45% of operators now offer at least one zero-rated app”, *Fierce Wireless* 15 July. Available from: http://www.fiercewireless.com/europe/story/report-45-operators-now-offer-least-one-zero-rated-app/2014-07-15 [30 June 2015].

Mullin, J 2015, “The Sunday Times sends DMCA notice to critics of Snowden hacking story”, *Ars Technica* 16 June. Available from: http://arstechnica.com/tech-policy/2015/06/sunday-times-sends-dmca-notice-to-critics-of-snowden-hacking-story/ [30 June 2015].

Nielsen 2014, Content is King, But Viewing Habits Vary by Demographic, 3 December 2014. Available from: http://www.nielsen.com/us/en/insights/news/2014/content-is-king-but-viewing-habits-vary-by-demographic.html [30 June 2015].

Nowak, P 2010, “Rogers lowers download limits as Netflix looms”, *CBC News* 22 July. Available from: http://www.cbc.ca/news/technology/rogers-lowers-download-limits-as-netflix-looms-1.950186 [30 June 2015].

Olson, P 2014, “The Quantified Other: Nest And Fitbit Chase A Lucrative Side Business”, *Forbes* 17 April. Available from: http://www.forbes.com/sites/parmyolson/2014/04/17/the-quantified-other-nest-and-fitbit-chase-a-lucrative-side-business/ [30 June 2015].

Palfrey, J & Zittrain, J 2011, “Better data for a better Internet”, *Science* 334, no. 6060, pp. 1210-1211.

Pasternack, A 2012, “NASA's Mars Rover Crashed Into a DMCA Takedown”, *Motherboard* 6 August. http://motherboard.vice.com/blog/nasa-s-mars-rover-crashed-into-a-dmca-takedown [30 June 2015].

Pélissié du Rausas, M. Manyika, J, Hazan, E, Bughin, J, Chui, M, & Said, R, 2011. “Internet Matters: The Net's Sweeping Impact on Growth, Jobs, and Prosperity”, McKinsey & Company. Available from: http://www.mckinsey.com/insights/high_tech_telecoms_internet/internet_matters [30 June 2015].

Ramirez, E 2014, “How to Download Minute-by-Minute Fitbit Data”, *Quantified Self* 26 September. Available from: http://quantifiedself.com/2014/09/download-minute-fitbit-data/ [30 June 2015].

Russell, J 2013, “Facebook’s ‘Every Phone’ app for feature phones passes 100 million monthly active users”, *The Next Web* 22 July. Available from: http://thenextweb.com/facebook/2013/07/22/facebooks-every-phone-app-for-feature-phones-passes-100-million-monthly-active-users/ [30 June 2015].

Saltzer, JH, Reed, DP & Clark, DD 1981, “End-to-End Arguments in System Design”, in *Proceedings of the Second International Conference on Distributed Computing Systems*, Paris, France, IEEE Computer Society, pp. 509-512.

Schneier, B 2012, Feudal Security. 3 December 2012 *Schneier on Security*. Available from: https://www.schneier.com/blog/archives/2012/12/feudal_sec.html [30 June 2015].

Schneier, B 2013, “You Have No Control Over Security on the Feudal Internet”, *Harvard Business Review* 6 June. Available from: https://hbr.org/2013/06/you-have-no-control-over-s [30 June 2015].

Segan, S 2015, “CDMA vs. GSM: What's the Difference?”, *PC Mag* 6 February. Available from: http://www.pcmag.com/article2/0,2817,2407896,00.asp [30 June 2015].

Sennett, R 2008. *The Craftsman*, Yale University Press, New Haven.

Seltzer, W 2010, “Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects of the DMCA on the First Amendment”, *Harvard Journal of Law and Technology*, vol. 24, no. 1, pp.171-232.

Siegrist, J 2015, LastPass Security Notice. 15 June 2015, Updated 16 June 2015. *LastPass Blog*. Available from: https://blog.lastpass.com/2015/06/lastpass-security-notice.html/ [30 June 2015].

Singel, R 2011, “Comcast Bans Seattle Man from Internet for His Cloudy Ways”, *Wired* 13 July. Available from: http://www.wired.com/2011/07/seattle-comcast/ [30 June 2015].

Sohn, D & McDiarmid, A 2010, Campaign Takedown Troubles: How Meritless Copyright Claims Threaten Online Political Speech, Center for Democracy and Technology. Available from: https://www.cdt.org/files/pdfs/copyright_takedowns.pdf [30 June 2015].

Tinholt, D 2013, “The Open Data Economy: Unlocking Economic Value by Opening Government and Public Data”, Capgemini Consulting. Available from: http://ebooks.capgemini-consulting.com/The-Open-Data-Economy/ [30 June 2015].

T-Mobile 2014, T-Mobile Sets Your Music Free, 18 June 2014. Available from: http://newsroom.t-mobile.com/news/t-mobile-sets-your-music-free.htm [30 June 2015].

Weber, M 1947, *The Theory of Social and Economic Organization*, Oxford University Press, New York.

Winner, L 1980, “Do Artifacts Have Politics?”, *Daedalus*: 121-136.

Van Schewick, B 2010, *Internet Architecture and Innovation*. MIT University Press, Cambridge.

Wall, M. 2015, “Facebook's Mark Zuckerberg hits back in Internet.org India row”, *BBC News* 17 April. Available from: http://www.bbc.com/news/technology-32349480 [30 June 2015].

Wolfson, T 2014, *Digital Rebellion: The Birth of the Cyber Left*. University of Illinois Press, Illinois.

Wu, T 2003 “Network Neutrality, Broadband Discrimination”, *Journal on Telecommunications & High Tech Law*, vol. 2, pp. 141-176.

Wu, T 2011, *The Master Switch: the Rise and Fall of Information Empires*, Vintage Books, New York.