Journal of
PEER PRODUCTION

NEW PERSPECTIVES
ON THE IMPLICATIONS
OF PEER PRODUCTION
FOR SOCIAL CHANGE

ISSUE #9
September 2016

ALTERNATIVE INTERNETS

PREVIEW

THE FULL PAPERS ARE AVAILABLE AT:
http://peerproduction.net/issues/issue-9-alternative-internets/

JOURNAL OF PEER PRODUCTION
ISSUE 9: SEPTEMBER 2016

SPECIAL ISSUE EDITORS:
FÉLIX TRÉGUER (ISCC-CNRS),
PANAYOTIS ANTONIADIS (NETHOOD),
JOHAN SÖDERBERG (GÖTEBORGS UNIVERSITET)

GRAPHIC DESIGN: LUISA LAPACCIANA
SET IN OPEN SANS BY STEVE MATTESON
UNDER APACHE LICENSE, VERSION 2.0
AND MIRIAM LIBRE BY MICHAL SAHAR
UNDER OPEN FONT LICENSE

THIS PREVIEW VERSION INCLUDES ONLY FRAGMENTS
OF THE PUBLISHED PAPERS. FULL VERSIONS ARE AVAILABLE AT:
http:///peerproduction.net/issues/issue-9-alternative-internets/

THE DESIGN AND PRINTING OF THIS PREVIEW WAS KINDLY
SUPPORTED BY NETCOMMONS, AN EU HORIZON2020 (CAPS)
PROJECT, NO. 688768. http:///netcommons.eu

THIS SPECIAL ISSUE ORIGINATED IN THE ALTERNET SEMINAR
(LONDON, 15-16 SEPTEMBER 2014). FOR MORE INFORMATION
AND INSPIRATION, YOU MAY REFER TO:
http:///www.iscc.cnrs.fr/spip.php?article1912

SPECIAL ISSUE EDITORS' INTRODUCTION

PEER REVIEWED ACADEMIC PAPERS

EXPERIMENTAL FORMAT

A FEW WORDS FROM OUR REVIEWERS

Alt. vs. Ctrl.

Editorial notes for the JoPP issue on Alternative Internets

The hopes of past generations of hackers weigh like a delirium on the brains of the newbies. Back in the days when Bulletin Board Systems metamorphosed into the Internet, the world's digital communications networks – hitherto confined to military, corporate and elite academic institutions – were at grasping reach of ordinary individuals. To declare the independence of the Internet from nation states and the corporate world seemed like no more than stating the bare facts. Even encrypted communication – the brainchild of military research – had leaked into the public's hands and had become a tool wielded against state power. Collectives of all stripes could make use of the new possibilities offered by the Web to bypass traditional media, broadcast their own voice and assemble in new ways in this new public sphere. For some time, at least, the Internet as a whole embodied "alternativeness."

Already by the mid-nineties, however, states began to reshape the communications infrastructure into something more manageable. Through a series of international treaties, legislations and market developments, ownership over this infrastructure was concentrated to a few multinational companies (McChesney, 2013). On top of this legal and technical basis, a new breed of informational capitalism sprang up, where value is siphoned from deterritorialized "open" flows (Fuchs, 2015). Meanwhile, the ecological footprint of communication technologies has come to represent a formidable challenge (Flipo et al., 2013).

It is in the light of these transformations that the emancipatory promises inherited from the 1980s and 1990s must be assessed. With every new wave of high-tech products, these promises have been renewed. For instance, when WiFi-antennas were rolled out in the 2000s, community WiFi-activists hoped to rebuild the communications infrastructure bottom-up (Dunbar-Hester, 2014). With the advent of crypto-currencies, some claimed to believe that bankers' control over global currency flows would be demolished (Karlström, 2014). The technology at hand might be new, but the storyline bundled with it is made up of recycled materials. It basically says: "Technology X has leveled the playing field, now individuals can outsmart the combined, global forces of state and capital."

Underlying this claim is a grander narrative about (information) technology as the harbinger of a brighter future. Although progressivism goes all the way back to the Scientific Revolution, it was given a particular, informational twist during the Cold War. In the 1950s and 1960s, disillusioned US Trotskyists – most notably among them Daniel Bell – rebranded historical materialism as the post-industrialism hypothesis. With this remake of hist-mat, history did no longer culminate in socialism, but in a global consumer village. Furthermore, the motor of transition was not class struggle anymore, but the inert development of technology (Barbrook, 2007). Though a spark of conflict has of course survived in the post-industrial hypothesis, this technological determinism flares up anew every time hackers and Internet activists rally behind, say, the inevitable demise of copyright or the awaiting triumph of decentralised communication networks (Söderberg, 2013). Determinism is performative, and never more so than when it is mobilized in political struggles.

This observation points to the instability of the meanings invested in computers and in the Internet itself. It suffices to recall the twin roots of these technologies, one in the military-industrial complex (Agar, 2003, Edwards, 1996), the other in the counter-culture and peace movement (Turner, 2006; 2013). The same undecidedness prevails today, as exemplified by the global controversies unleashed by NSA whistleblower Edward Snowden. The documents leaked by Snowden revealed the extent to which communications surveillance has been built into the pipes of a supposedly flat network, giving rise to unprecedented mobilisations aimed at resisting it. But paradoxically, this wave of resistance is now leading to the legalisation of mass surveillance (Tréguer, 2016).

Because of these persistent ambiguities, it would be as wrong to denounce the inherent oppressiveness of the Internet as it would be to celebrate the alternative essence of this technology. Either position amounts to the same thing: A foreclosing of the struggle in which the future meaning of the technology is determined. Both Alt. and Ctrl. are possible and competing scenarios. They evolve in constant interaction.

How can we, as scholars and/or activists, sort out this complexity and make an assessment of the balance of forces, while reinvigorating hope for the future? Can we learn from the past to ward off the eternal return of a dystopian future? Posing these questions – and perhaps contributing to answers – is the task that we have set for ourselves in this special issue of *Journal of Peer Production* on "alternative Internets."

If the meaning of the "Internet" is instable, then the definition of "alternative" in "alternative Internets" is even more so. Alternativeness is never an absolute. It is relative to something else, the non-alternative, which must also be defined. In this respect, Paschal Preston notes that alternative Internets were found in online applications that "manage to challenge and resist domination by commercial and other sectional interests", in particular those "operating as alternative and/or minority media for the exchanges of news and commentary on political and social developments which are marginalized in mainstream media and debates" (Preston, 2001). Likewise, Chris Atton writes that alternative Internets are "produced outside the forces of market economics and the state" (Atton, 2003). As seen from these rather conventional definitions, alternativeness is measured in distance from the centres of state and capital.

How can we move past the couple of "useful others" (the state, the market) to better grasp alternativeness? The tools, applications and media that form part of the Internet can be assessed as composites made up of different dimensions. Some important parameters include the underlying funding and economic models, the governance schemes for taking decisions and allocating tasks, or the modes of production. Nick Couldy puts emphasis on this latter dimension when discussing alternative online media, stressing that the most important for them is to challenge big corporate mass media by overcoming "the entrenched division of labour (producers of stories vs. consumers of stories)" (Couldry, 2003:45).

Another crucial line of inquiry for evaluating an alternative Internet relates to the underlying content or ideology that it circulates. For Sandoval and Fuchs, this is the most important dimension, and anything claiming to be alternative must adopt a critical stance to "try to contribute to emancipatory societal transformation" and "question dominative social relations" (Sandoval & Fuchs, 2009). When we consider the Internet, ideology is found in the values that underly the design of a technology or application, structure its uses or populate the online social space that this application brings about.

Of course, ideology is also embedded in the discourses and practices of the many actors trying to influence its development at the technical, social or legal level. The Internet is indeed a social space made up of a myriad of contentious actors such as hackers, software developers and makers who hack, code and make, of advocacy groups with their value-ridden proclamations and legalese, of Internet users making claims to an enlarged citizenship, and of course of all the entrepreneurs, crooks, bureaucrats, agents provocateurs and politicians they fight against or – less often – coalise with. All of these actors produce, use or advocate for particular technologies, fight against or encourage dystopic trends, work towards or oppose emancipatory projects, and in doing so produce political discourses and imaginaries that weigh on the social construction of the Internet. As such, they are part of our field of inquiry when we talk about "alternative Internets." Their own contradictions further complicate the analysis. A protagonist might go to bed as a subversive hacker but wake up the next day as a piece-rate worker in someone else's pension plan, or worse.

This speaks to the more general fact that a socio-technical *dispositif* that is "alternative" on one level tends to be preconditioned by status quo on some other level. For instance, openness in terms of software licenses often comes hand in hand with a closure in terms of technical expertise. To put it in more general terms, the alternative, if it is to be effective, is necessarily compromised by the dominant. Here as elsewhere, a maximising strategy is paralysing: As the proverb goes, "the perfect is the enemy of the good." In this spirit, Marisol Sandoval and Christian Fuchs have argued for "politically effective alternative media that in order to advance transformative political can

include certain elements of capitalist mass media" (Sandoval & Fuchs, 2009:147). According to the authors, subscription fees or even advertising might be required if a project is to break out of the niche to reach a broader audience. Assessing trade-offs is part of the alternative game.

In this issue of the JoPP, we present contributions that explore these questions and shed light on the blind spots of alternative Internets.

With "**In Defense of the Digital Craftsperson,**" ***James Losey*** and ***Sascha D. Meinrath*** offer a conceptual framework for analyzing control in Internet technical architectures along five dimensions: networks, devices, applications/services, content, and data. By updating prior analysis regarding threats to communicational autonomy and to the ability to tinker with digital technologies, they identify key challenges and help think systematically about strategies of resistance.

Stefano Crabu, ***Federica Giovanella***, ***Leonardo Maccari***, and ***Paolo Magaudda*** consider the bottom of the "network" layer of Losey and Meinrath's framework by offering an interdisciplinary perspective on Ninux, a network of wireless community networks in Italy. Their paper, "**Hacktivism, Infrastructures and Legal Frameworks in Community Networks: the Italian Case of Ninux.org**", benefits from the active participation of one of the authors in Ninux, and presents interesting evidence about the limited levels of decentralization in a network built exactly around this vision. It is also one of the very few papers that brings insights on the legal aspects of community networks, focusing on the question of liability and different organizational forms that can protect these networks against legal actions.

Christina Haralanova and ***Evan Light*** offer an insider's look at a much smaller community network in Montreal, called Réseau Libre. In their paper entitled "**Enmeshed Lives? Examining the Potentials and the Limits in the Provision of Wireless Networks,**" they try to understand two other important contradictions in community networks. First, they examine their possible role as both an "alternative Internet provider," as well as an "alternative to the Internet all together," that is to say a local infrastructure providing local services for the members of the network. They also identify the lack of adequate security against surveillance, despite the fact that many people cite enhanced privacy and security options as a reason for their participation in the community. As the paper shows, even though they might foster knowledge-sharing around issues such as computer security, these networks remain "as insecure as the Internet itself."

The paper "**Going Off-the-Cloud: The Role of Art in the Development of a User-Owned & Controlled Connected World**" by ***Daphne Dragona*** and ***Dimitris Charitos*** also explores various alternatives of user-owned network infrastructures, this time focusing on an "alternative to the Internet all together", imagined and experimented by artists and activists. The scale here is much smaller, with most networks comprised by a single wireless router acting as a hotspot allowing only local interactions between those in physical proximity. Such "off-the-cloud" networks, have been given numerous telling names like Netless, PirateBox, Occupy here, Hot probs, Datafield, Hive networks, Autonomous Cube. According to the authors, these and many more similar inspiring projects work towards "new modes of organization and responsibility (...) beyond the sovereignty of the cloud."

In "**Gesturing Towards 'Anti-Colonial Hacking' and its Infrastructure,**" ***Sophie Toupin*** draws on a historical example to investigate the opportunities and limitations for appropriating cryptography today. Her interviews with some of the key actors in this glorious moment of hacker politics is particularly inspiring, as is Toupin's willingness to expand our understanding of "hacktivism" by looking beyond Europe and North America.

Primavera De Filippi's piece focuses on "**The Interplay between Decentralization and Privacy,**" using blockchain technologies as a case-study. She shows that while decentralized architectures are often key to the design of alternative Internets, they come with important challenges with regards to privacy protection. Her critical assessment is particularly timely, as blockchain technologies are rapidly co-opted by the bureaucratic organizations there were originally meant to subvert.

In "**Finding an Alternate Route: Circumventing Conventional Models of Agricultural Commerce and Aid,**" ***Stephen Quilley***, ***Jason Hawreliak*** and ***Katie Kish*** present a case study on Open Source Ecology (OSE). OSE started in the United States but has sprouted similar initiatives in Europe and South America. It is now developing a series of open source industrial machines and publishes the designs online. One of the primary goals of OSE is to provide collaboratively produced blueprints for relatively inexpensive agricultural machinery, such as tractors, backhoes, and compressed earth brick presses for constructing buildings. The authors argue that the proliferation of open source networks can reshape domains that have traditionally relied on state and inter-state actors such as international aid.

Lastly, ***Melanie Dulong de Rosnay***'s experimental text on "**Alternative Policies for Alternative Internets**" raises awareness on the importance of the terms of use of Internet platforms. By quoting numerous such policies – from both mainstream and alternative platforms – on topics like copyright or data protection, she manages to create a diverse mix of feelings, all the way from anger to laughter. Most importantly, this collection warns us about the legal issues that alternative platforms have to deal with, and provides inspiration and useful information on how to address them in practice.

Each of these papers addresses one or more of the "layers" described by Losey and Meinrath, analysing different facets of alternativeness. But there are other dimensions outside this framework that we have not touched upon. For instance, although the issue deals with low-tech practice, the staggering ecological impact of Internet technologies and their environmental unsustainability is not addressed, despite the growing attention of scholars and engineers to these crucial issues (Chen, 2016). Although two papers focus on urban community networks, other aspects of the urban dimension of alternative Internets are overlooked. Together with the notion of locality, urbanity appears to be crucial in helping actualise the potential of alternative Internets to become autonomous infrastructures operating outside the commercial Internet. It is also an avenue to think about resistance strategies: As the urban space becomes increasingly hybrid and renders the digital and physical evermore intertwined, those movements fighting for the "right to the city" (Lefebvre, 1996) and those working towards the "right to the Internet" will have renewed opportunities to join forces (Antoniadis & Apostol, 2014).

For sure, advancing alternative Internets will require from a very diverse set of actors to go beyond traditional boundaries so as to engage in effective collaboration. In academia too, transdisciplinary research – though still in its infancy – is extremely promising. We hope that this issue of the JoPP will be read as an invitation to work further in that direction.

As editors, we would like to thank Bryan Hugill for helping us copy-edit the papers, and express our gratitude to both authors and reviewers. We hope that readers will be as inspired as we are by these very diverse contributions, which each in their own ways point towards a more democratic and more inclusive Internet.

Félix Tréguer,
Panayotis Antoniadis,
Johan Söderberg

James Losey and Sascha D. Meinrath

In Defense of the Digital Craftperson

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

The increasingly centralized control of communications technologies is limiting 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). By updating prior theorizing (Burns 2003; Lessig 2002; Benkler 2006; Zittrain 2008), this paper offers a framework for analyzing control along 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 Craftspersons.

KEYWORDS: *Internet-of-things, Internet Architecture, Network Commons, DRM, Remixing, 21st Century Ownership, Privacy, Digital Feudalism.*

INTRODUCTION

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 software have supported continuing innovation and creative destruction (Schumpeter 1942). Fundamentally, this "permissionless" Internet supported the craftspersonship 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 (Sennett 2008). However, contemporary business practices are shifting us away from this historical precedent and instituting ever-increasing centralization of control over communications technologies. The networking of everday objects — from thermostats, to cars and home appliances, to toys – begs the question: do these computing devices enable end-users innovation, or serve as centrally controlled constraints? ///////

/// 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 analyzes the impact of the tensions of five conceptual layers of this global network. ///

/////// We posit that different technological layers can be leveraged for political or commercial interests to limit functionality and innovation across the entire technology stack. This framework provides a new methodology for examining how the locus of control supports and/or undermines craftspersonship across five dimensions of networked information and communications technology (ICT): networks, devices, applications/services, content, and data. 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 Craftspersonship that will create more liberatory future innovations. ///////

/// Although not every user will necessarily offer innovations, and not at all times, the potential for craftspersonship defines the innovative potential of the Internet and offers a framework for understanding the implications of the architecture of networked systems. ///

CONCLUSION

Over the next decade, the number of networked devices is expected to grow by an order of magnitude. By 2015, the Internet connected over 8 billion devices around the globe – more than one per person; Cisco projects that by 2020 there will be 6.5 Internet connected devices for every person on the planet (Evans 2011). However, the locus of control over networks, devices, applications, content, and data will determine the extent that Digital Craftspersonship will continue to thrive. ///////

/// Digital Craftspersonship is an ideal that can serve as a benchmarch for public policy decision-making, especially for policy makers that want to promote the Internet as a platform for economic opportunity. ///

/////// Legislation and regulations that impact each layer of a technology stack should be evaluated to determine whether they increase or reduce the potential for craftspersonship. The establishment of network neutrality rules in the United States, and resistance to an application-restricted "Internet" in India, demonstrate positive steps forward for preserving network-layer craftspersonship. However, the use of copyright to shift the concept of "ownership" of everyday goods – from cars to coffeemakers – illustrates how companies are exerting control over goods in fundamentally new ways, necessitating updates to traditional consumer protections. Additionally, control of personal information continues to be a growing policy predicament. ///////

/////// Entrepreneurs, policy makers, and careful and critical observers must look beyond their surface-level understanding of technology and interrogate the technological underpinnings of contemporary and future digital technologies. The overarching positive and negative repercussions of technological innovations are increasingly not silo-ized, but can only be understood in relation to the larger digital ecosystem in which they reside.///////

/// We provide a parsimonious framework for understanding how the politics within and amongst technological layers of networked systems change the relationship between users, owners, and digital technology.///

/////// This framework focuses on the relationship between users and the networked communications tools they utilize. And the future of digital craftspersonship will pit the liberatory potential of 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 will become digital serfs facing an ever-more-oppressive panoptic and data extractive networked world. ///////

Stefano Crabu, Federica Giovanella, Leonardo Maccari, Paolo Magaudda

Hacktivism, Infrastructures and Legal Frameworks in Community Networks

the Italian Case of Ninux.org

Community Networks (CN) are an emerging world-wide phenomenon that is receiving growing attention from a number of different disciplines. A CN is an infrastructure for digital communication, an alternative to the mainstream approach of commercial Internet Service Providers (ISPs). The paper starts by describing the phenomenon of the CNs; sketching its historical development, the motivations underlying the foundation and use of these networks, their functioning and main legal implications. This introduction is followed by an examination of the specific case of Ninux.org, looking at practices, discourses, and interactions among activists participating in the project. On the basis of this analysis, the paper moves on to consider some technical characteristics and specifications of the network, revealing how the technological infrastructure only partially realizes an effective decentralization and horizontal organization of the network.

KEYWORDS: *Wireless community networks, decentralization, Italy, hacktivism, distributed infrastructures.*

INTRODUCTION

/////// This paper investigates the experience of an Italian CN called Ninux.org, exploring the discourses and politics developed within the community around the project and analysing how these cultural and social dimensions are effectively translated into the technical construction and topology of the network. ///////

/////// Inspired by Science & Technology Studies (Latour 2004) and their aim at disentangling the articulation between the technical, the discursive and the social dimensions of socio-technical phenomena, the paper is intended to reveal arrangements and misalignments that characterize the Ninux.org network infrastructure. Methodologically, the article summarizes the results of a research project carried out by a multidisciplinary team of scholars from the social sciences, computer engineering and law. The heterogeneity of the fields involved is reflected directly in the distinct perspectives that emerge from the analysis, in the multiple research methodologies adopted and also in the resultant variety of data presented and discussed. These data include qualitative interviews with participants in the network, a topological analysis of the infrastructure flows, data on participation in the collective mailing list and an analysis of the Italian laws on bottom-up communication infrastructures. ///////

/// The sharing of a coherent, but constantly evolving, set of political views about the increasing centralization of the Internet is a vital driver of participation and is crucial to successful collective negotiations around the shape of the whole infrastructure. ///

/////// The article starts with an introduction to the technical features of a wireless CN or “mesh network”, highlighting the specific properties that distinguish them from home Wi-Fi or larger networks. We present a quick historical outline of these networks, and a review of the recent literature on the social and legal concerns related to them. Then we move to the case of an Italian wireless CN called Ninux.org, tracing its development from 2001 to its recent expansion. After a description of the evolution of the network, the article presents a detailed analysis of three specific levels of the Italian CN, reflecting the three distinctive analytical perspectives adopted in the research. ///////

CONCLUSIVE REMARKS AND FUTURE WORK

/////// It is easy to be fascinated by a new technology that has a bottom-up approach and seems to propose a viable alternative to an existing, and controversial, technology. But enthusiasm for this new ‘liberation technology’ is often marred by the ambivalence of the political ideals that inspired it, an overestimation of the technical decentralization achieved, or simply by a complete lack of any understanding of the legal sustainability of the proposed model. ///////

/// The multidisciplinary approach adopted in this research contributes to the expansion of the existing body of research on CNs and to the widening of our understanding of how political and cultural views and technical and infrastructural issues need to be continuously realigned and re-framed. ///

///////// According to Ninux activists decentralization and distribution seem to be the key differences from mainstream providers that would guarantee the CN`s development as an “alternative Internet”. However, our technical analysis has shown that just “being distributed” does not guarantee that a CN is effectively different from a hierarchical, traditional network. We have shown that the mobilization of activists and participants, when combined with the intrinsic difficulties related to the bottom-up construction of a network, does not automatically/necessarily generate an effectively decentralized infrastructure for Ninux.org. ///////

///////In fact, the network has evolved with inconsistencies that are not introduced “by design”, as in traditional networks, but emerge spontaneously from the project. One such inconsistency is the fundamental role played by certain network nodes, another is the fact that discussions in the mailing lists are generally led by a small core group of people. Moreover, from a legal point of view, this concentration of responsibilities (despite being informal, and not explicitly assigned) weakens the network. ///////

/// More broadly, the picture that emerges from this multidisciplinary analysis of the Italian wireless CN Ninux.org is closely linked to the multidimensional factors that together have shaped the emergence of this alternative network. ///

/////// Indeed, the forms of members participation cannot be understood without reference to the actual infrastructure topology; at the same time, understanding the whole set of political assumptions supporting the project is crucial to the expansion of the CN, both in terms of participant numbers and of the network’s physical growth; finally, the potential legal liabilities to which these networks are exposed must be considered in any vision of the future development of the project. /////////

ACKNOWLEDGMENTS

This work was financed partially by the University of Trento under the grant “Wireless Community Net-works: A Novel Techno-Legal Approach” - Strategic Projects 2014, and partially by the European Commission, H2020-ICT-2015 Programme, Grant Number 688768 ‘netCommons’ (Network Infrastructure as Commons). ///////

Christina Haralanova and Evan Light

Enmeshed lives? Examining the potentials and the limits in the provision of wireless networks

The case of Réseau Libre

Mesh networks in urban spaces are on the rise and are increasingly widespread and innovative. Often built by people with an interest in community networks and the distribution of power and control within the Internet, mesh networks make for a fascinating phenomena to research in the ways they bridge the social and the political. This article presents a study of Réseau Libre, an emerging mesh network community in Montréal. Started in 2012 by a group of tech activists, its original goal was to connect peers through an independent, self-funded and decentralized wireless network. By creating an autonomous long-range wireless network outside the scope of government regulation. Réseau Libre's project is inherently political and within the creeping reaches of the surveillance state, seen as increasingly necessary. In this article, we examine the history and organization of Réseau Libre, its organizational limits and physical realities. We analyze the project within its particular political context and provide a number of recommendations oriented around the future success of Réseau Libre and other similar projects around the world.

KEYWORDS *Mesh networks, surveillance, community networks, network security, Internet alternatives.*

FRAGMENTS

/////// In the current context of post-Snowden era of mass surveillance and monopolized telecommunications, it is essential to closely examine the alternative solutions offered by local grassroots tech organizations working to make public goods accessible to their immediate communities. ///////

/////// We examine a developing Montreal-based mesh network, Réseau Libre[1], which emerged during Quebec's "Maple Spring" protests[2] and the Montreal offshoot of the Occupy Wall Street movement, Occupy Montreal[3], and began serious development during the initial Snowden revelations. ///////

/////// Réseau Libre is not the first project in Quebec intending to bring WiFi connectivity to the masses. ///////

/////// The idea to start an independent mesh network in Montreal originated with a few individuals and organizations who had been working separately on mesh, WiFi, or local Internet access projects. ///////

/// Today, Réseau Libre represents a community of technologically apt individuals interested in wireless networking and free and open-source software. ///

/////// Réseau Libre has been created based on activist principles of Internet freedom and independence from monopolized telecommunications infrastructure. ///////

/////// Mesh networks such as Réseau Libre are examples of local communities organizing against monopolized infrastructure by using consumer-grade technology to build distributed networks.///////

/// If I want to access a database at my university library or a file at city hall or on my friend's computer, why should I have to pay an intermediary to do so? ///

/////// We approach our study through a qualitative analysis of interviews with members of the Réseau Libre mesh network, these providing us with personal background information and multiple perspectives on the history of the network.///////

Our method aims to bring forward the personal trajectories of certain key participants, founders and developers of the mesh network.

We relate strongly to Sandvig's proposition that community networks should be examined according to their own unique set of conditions and thus aim to interpret the history and current state of Réseau Libre according to his four points of analysis: infrastructure, autonomy, professionalization, learner community (2012).

/////// The desire for building an alternative network of users, independent from the Internet, comes with the concern of how to get a critical mass of users to manage to connect everyone throughout the city, and for the project to grow and thrive without outside support.///////

/////// In one way or another, Réseau Libre represents an example of professionalization, either as a new field of exploration made possible through inexpensive hardware and open standards, or through the building of a network that allows users to explore wireless networking in their own way, and adapt it to their personal needs. For most study participants, such an acquisition of new knowledge and skills is of great personal and professional benefit. ///////

/// "I don't know what to do with Réseau Libre yet… for now it's a platform for experimentation by a bunch of a geeks"///

/////// Network security of Réseau Libre is conceived of in two conflicting ways. First, there is no security in terms of your information being safe and second, the security of the network infrastructure in and of itself relies on human relationships and it is these trust relations that are then grafted onto the network links.

CONCLUSIONS / RECOMMENDATIONS

1. Privacy practices yet to come.
Réseau Libre, while using software and hardware produced by others, has paid more attention to the technical aspects of their network design than the social aspects and are thus at an impasse. At this critical juncture wherein the public-at-large is informed to some degree about mass surveillance and increasingly cares about personal privacy, Réseau Libre has the opportunity to integrate privacy practices into the foundation of their network and make it a core facet of their public identity.

2. Step up to the policy plate!
To take advantage of the opportunity to intervene in the spaces of privacy and digital infrastructure, we recommend that Réseau Libre engage more broadly with technical development and policy debates. By intervening in public venues and processes, one leaves a public record and presents examples of alternative methods to both those in power and others who may look to you for a model or who may be in a similar or earlier stage of organizational development.

3. Evolution in the practices of independent media. Réseau Libre does so by providing a space not unlike those created by community radio and television stations and community newspapers – but a space for physical, technical and philosophical experimentation.

1 *http://reseaulibre.ca*
2 *The Maple Spring was a 7.5 month long student strike in Quebec that morphed into broader protests over freedom of expression and government corruption. The student strike lasted from February 13, 2012 to September 7, 2012.*
3 *http://www.occupons-montreal.org/*

Daphne Dragona and Dimitris Charitos

Going off-the-cloud

The role of art in the development of a user-owned & controlled connected world

During the last fifteen years, while everyday life is being increasingly datafied, an emerging scene of network practitioners from different fields has been actively involved in building alternative networks of communication and file-sharing. Among the practitioners of this DIY networking scene, a growing number of artists has been playing a crucial role in offering alternatives and critical perspectives. The aim of this paper is to present and discuss these particular initiatives in relation to the needs of the different time-periods that they emerged in.

/////// The networked world is a world of opacity and this is gradually becoming one of the fundamental asymmetries in the manner that users relate to the networks. Artist Julian Oliver (2014) suggests that "without edges we cannot know where we are nor through whom we speak", while artist Danja Vasiliev (2014) also remarks that "we hardly know what our device does behind our back".

Reaching the point where 'the internet does not exist' (Aranda et al. 2014), where all we know is the presence of the Cloud, new facts need to be taken into consideration. When technology is becoming invisible, we as users at the same time are losing our rights on it. ///////

/// what Greenfield has also framed as a need for translators, for "people capable of opening these occult systems, demystifying them and explaining their implications" to the others.///

/////// Building their own infrastructures by using open hardware and software, they have been developing and communicating models that can be considered as current 'counter-infrastructures' (Dragona 2014) that aim to provoke change of a bottom-up structure. Community networks, ad hoc offline networks and local WiFi access points are examples of such infrastructures that users themselves can own, manage and control. ///////

///this paper presents and discusses a series of appropriately selected alternative DIY networks, platforms and initiatives that are being proposed by artists as a response to today's datafied and controlled connected world. ///

//////The fundamental idea behind DIY networking is that it offers its users the possibility of ownership of the infrastructure as well as of all generated digital information. *(Antoniadis & Apostol 2014)* //////

"The sleeping beauty of mesh has been kissed into life by the community" *Elektra (Medosch 2015)*

/////// The need to connect offline is not new. Well known mesh networks such as the Spanish Guifi, the German Freifunk, the Austrian Funkfeuer and the Athenian AWMN, established their first urban mesh nodes and links in the first half of the last decade. While, at the beginning, their popularity grew thanks to the greater speed that these connections offered, soon it became clear that the potentiality and the outreach of these networks could go far beyond that. //////////

/// Consume.net /// Freifunk/// Funkfeuer /// Sarantaporo.gr /// Valparaiso Mesh///

/// Apart from being initiators, artists in the last decade were also invited to use and animate networks in order to communicate their advantages to the citizens.///

/////// In these cases it is important to remember that free connectivity and communication among inhabitants was meant to build not only an infrastructure after their needs, but also strong links among the members of the community and a sense of shared responsibility for its maintenance. ///////

/////// the word 'tactical' is considered more appropriate, as it implies the need and the intention behind the deployment of such networks. This term also clarifies how tactical mesh networks differ from community mesh networks, although they often share the same infrastructure. ///////

/// Fluid Nexus /// Qaul.net /// Dead Drops /// Deadswap /// r15n

/// With the term 'off-the cloud', we wish to discuss a new constellation of offline WiFi access points, sharing networks, autonomous mesh networks, personal servers and syncing platforms that together not only bring in alternative infrastructures but also communicate to users the essential new forms of literacies needed for using and appropriating them. In other words, it is not only about sharing and storing data safely and locally but also about knowing how to set up the system, how to use it, maintain it, control it and own it. ///////

///"off-the-cloud" toolkits are by their nature open, gaining the life and the features that their owners want them to gain. ////

///Hive Networks/// Subnodes///

Hot probs /// Occupy Here/// PirateBox///Datafield/// Superglue ///Dowse ///

/////// Often with a speculative character, but yet again functional, these projects discuss issues of surveillance and the possibilities for users' empowerment over networked infrastructures.

/// Autonomous Cube /// Sylloge of Codes /// Netless /// Right to Flight /// Electronic Countermeasures /// Panda to Panda ///

/////// Objects are repurposed in order to serve offline connectivity. When asking how artworks as such can provoke change, it is important to take into consideration the stance artists take when engaging with future scenarios. ///////

/////// Going "off-the-cloud" not only is a way of escaping data surveillance and commodification but it also assists in building new bonds among a community, in connecting in times of emergency, and in having control of one's data.///////

///the proposed infrastructures can be seen as part of the new 'Network Commons'///

/////// The forms of organization artists introduce as part of a DIY networking practice capture not only social and technological topologies but also experiences, languages, codes, driven we could say by affect. ////////

/////// Art's special contribution in DIY networking is to build awareness, to motivate and activate people towards change which -in the particular context- concerns systems of connectivity beyond the possibility of surveillance and control. By turning the attention again towards the user, by making the topologies and the infrastructures tangible and accessible and by allowing their further modification and use by their users and their communities, new modes of organization and responsibility are becoming apparent, beyond the sovereignty of the cloud./ //////

Sophie Toupin

Gesturing Towards "Anti-Colonial Hacking" and its Infrastructure

In the 1980s, freedom fighters and hackers from South Africa built an autonomous encrypted communication network that allowed activists infiltrated on the ground to communicate with the senior leadership of the African National Congress (ANC) based in Lusaka, Zambia via London. The encrypted communication network was set up as part of Operation Vula to attempt to launch a people's war and ultimately liberate a people's from apartheid. This article speaks to the history of technology in its attempts to further document and elucidate the encrypted communication network. To accomplish this, it draws both on previously available sources and also personal accounts obtained through interviews with some of the core individuals involved in the network's functioning. It also aims at expanding our understanding of highly intentional, politically-motivated practices of hacking, and the socio-technical infrastructures needed for such practices to exist.

KEYWORDS: *Anti-colonial hacking, Phreaking, Cryptography, Anti-Apartheid, South Africa, Infrastructure.*

INTRODUCTION

It is October 1989. Janet Love, a commander in the militant anti-apartheid organisation Umkhonto we Sizwe (MK), has infiltrated an office in Johannesburg and now sits anonymously, holding a small tape player next to a land-line phone. Earlier in the morning she had typed a message on a laptop computer bearing an encrypted floppy disk smuggled in a few months prior by a Dutch flight attendant named Antoinette, who doubled as an anti-apartheid operative. Completing the message, she enciphered it before passing it out through the computer's serial port to an acoustic coupler modem. The digital data was thus converted to sound, which she captured on a small cassette tape recorder—the same device she now holds up to the telephone receiver. On the other end, in London, the phone is connected to a special answering machine configured by freedom fighter and hacker Tim Jenkin with the express purpose of receiving just such a message from South Africa. Working on his computer, Jenkin plays the audio message back through an acoustic modem similar to the one used by Love, converting its analog signal back to digital—rendering it back into data that he can decipher using a floppy disk paired to the one used by Love. At the end of this process, a simple string of plaintext appears on Jenkin's computer screen. The message reads: "[...] We're awaiting a travel document for her. She's ready to leave at any moment. [...] Amandla!" Reading the message, Jenkin quickly intuits that it needs to be passed on to Lusaka, Zambia, where it can be seen by the senior leadership of the African National Congress (ANC). Jenkins repeats the encryption process and forwards the message along to Lusaka, where a Dutch anti-apartheid activist named Lucia receives the enciphered messages, deciphers it once more, and prints it out to hard copy. A courier picks it up and it is on its way to the senior ANC members. ///////

/////// This article will begin with some background on the struggles in South Africa (Holland 1989) at that time, contextualizing the reasons why an autonomous encrypted communication network (AECN) was seen as desirable in the first place. It is important to understand that the ANC already had a history of setting up different forms of communication systems, not only for strategic communication across borders, but also to share and distribute information more generally. These systems included radio broadcasts, newspapers, leaflet-bombs, and others, and their use was intended to inform, to trigger activism, and to inspire hope in South Africans who were experiencing oppression on a day-to-day basis. The appeal of a cryptographic network becomes further apparent when one considers the distance separating anti-apartheid activists, the exiled status of the ANC leadership, the high levels of counter-intelligence infiltration within the movement, and the burdensome nature of hand-written cryptography. Not to mention the apartheid regime's routine surveillance of phone calls, postal mails, leaflets, and radio broadcasts both inside and outside South Africa. Phone phreaking, programming, and cryptographic tools seemed ripe for use in advancing the political aims of Operation Vula. ///////

///The article will proceed with a discussion of four aspects of the AECN's infrastructure, each of which helps to illustrate the ways a politically-inclined hacking practice manifested in an anti-colonial context. I am drawing on the notion that "infrastructures are built networks that facilitate the flow of goods, people, or ideas and allow for their exchange over space (Larkin 2013)". Moreover, my use of the term "infrastructure" is not solely limited to material or technological components, but also socio-technological aspects. ///

///In this way, I hope to highlight not only the materiality of this communication practice but also its reliance on human agency, technological affordances, ethical principles of autonomy and solidarity, and more (Bowker & Star 2000; Parks & Starosielski 2015). ///

/////// The history of phone phreaking, hacking, and cryptography have had until now strong Western and American groundings (Coleman 2014a; Lapsley 2013; Levy 2002). While acknowledging the importance of these histories to the hacker and crypto movements today, I will nonetheless argue that the AECN is an example which enriches the history of phone phreaking, hacking, and cryptography. Not only does it elucidate the use of these practices' in an anti-colonial struggle, but it also shows the steps that were necessary to configure both technologies and social realities for use in a specific context and underground situation.

CONCLUSION

The encrypted communication network established that was set up as part of the ANC in its endeavour to end apartheid functions as an important example of the role hacking can play in an intentional political practice. By elucidating scenarios where phone phreaking, cryptography, and hacking were utilized in an anti-colonial setting, this article seeks to expand understandings of the possible goals, aspirations, and politics inherent to these practices. It also shows how the political functions of these practices cannot be understood as emerging solely from the technological aspects of such a communication network—instead, one must consider an expansive socio-technical infrastructure, composed of an assemblage of actors, technologies, and conditions, among other elements. ///////

Primavera De Filippi

The Interplay between Decentralization and Privacy

The case of blockchain technologies

This paper analyses the case of Bitcoin and other blockchain-based networks, as an example of decentralized infrastructures which suffers from radical transparency. While they provide a series of privacy benefits to end-users, the characteristics of these networks present both advantages and risks to the privacy of end-users. On the one hand, the pseudonymous nature of many blockchain-based networks allows for people to transact on a peer-to-peer basis, without disclosing their identity to anyone. On the other hand, the transparency inherent to these networks is such that anyone can retrieve the history of all transactions performed on a blockchain and rely on big data analytics in order to retrieve potentially sensitive information. The paper concludes that, in spite of the apparent dichotomy between transparency and privacy, there is no real conflict between the two. With the use of advanced cryptographic techniques, it is only a matter of time before people identify news ways to preserve individual privacy in decentralized architectures.

INTRODUCTION

In the wake of the Snowden revelations, there has been a great deal of debate around the need to protect the privacy and confidentiality of online communication. We can witness a growing interest in decentralized architectures as a way to protect one's privacy against the authority and surveillance of centralized third parties. As a general rule, in fact, decentralized architectures are perceived as being more supportive of individual freedoms and civil liberties, such as privacy and freedom of expression. Yet, decentralized systems are much more difficult to implement than centralized platforms. In order to allow for an effective coordination amongst a distributed network of peers, decentralized architectures generally rely on the disclosure of everyone's interactions. ///////

/// If the price of centralization is trust —as users need to trust centralized operators with their data, decentralization comes at the price of transparency —as everyone's interactions are made visible to all network's nodes.///

/////// In decentralized systems, surveillance is difficult to achieve (although not impossible) because there is no single entity that controls and manages the flow of information. Instead of storing personal data into central repositories operated by trusted third parties, decentralized solutions rely on a large number of peers, each hosting only a small chunk of data, which must all cooperate for the data to be processed by an authorized third party. In this sense, decentralization can reduce the power asymmetries that generally provide unfair advantages to centralized operators—with the drawback, however, of increasing coordination costs. ///////

/////// The more decentralized an infrastructure is, the less it relies on trust and the more it relies on transparency instead. On that regard, it is worth distinguishing between two types of transparency: content transparency, which requires the disclosure of the actual content of communication; and protocol transparency, which only requires the disclosure of metadata or other administrative information. While the former is not a prerequisite for decentralized coordination, the latter is needed in virtually all decentralized infrastructures. ///////

/// Privacy and Decentralization: friends or foes? The case of blockchain technologies ///

/////// A blockchain is as a secure database that comprises a public log of all transactions which have been thus far validated by the network. In view of its decentralized nature, the security of the blockchain and the validity of every transaction can only be ensured through distributed consensus (i.e. through nodes verifying the integrity and legitimacy of each block, independently of any trusted third party). ///////

/// The core innovation of the blockchain is its ability to validate transactions in a decentralized manner, without the need for a trusted authority. ///

/////// Blockchain technologies can significantly affect the existing power dynamics between online operators and their users. The transparency of every blockchain network provides a greater degree of control to end-users, who no longer need to trust online operators with regard to the software they run. Indeed, given that the software bytecode is deployed directly onto the blockchain, users can always look at it in order to better understand the inner workings of that software —knowing that no one can impose or even modify any of these technical rules without obtaining the consensus of the network. ///////

/// The inherent transparency of blockchain technologies represents a useful mechanism to coordinate the behavior of several individuals that do not know (nor trust) each other. ///

/////// However, such a degree of transparency might not always be desirable. In some cases, in fact, the transparency inherent to these decentralized technologies might actually go counter to the traditional expectations of privacy. ///////

/// On a blockchain, the history of every transaction can potentially be tracked down, back to the place where it originated. ///

/////// But while the blockchain does not, as such, provide any kind of privacy protection, it would be a mistake to believe that the transparency required to operate on the blockchain necessarily and unavoidably goes counter to the privacy of end-users. In spite of the apparently conflictual relationship that subsists between privacy and transparency, the two are not necessarily incompatible with each other. Transparency only subsists at the most basic layer of the blockchain —that which is responsible for applying the distributed consensus algorithm. ///////

///Additional layers of encryption and obfuscation can be built on top of the blockchain protocol, so as to conceal the source and destination of transactions, as well as potentially even the content thereof.///

/////// While ensuring that transaction data remains confidential by default, these advanced cryptographic techniques are not necessarily incompatible with the notion of transparency. Users retain the ability to uncloak their transaction data so as to disclose relevant information to third party, in a certified way.///////

CONCLUSION

Looking at the relationship between privacy and transparency in decentralized infrastructures, one can see that —although there obviously exists a correlation between them— the interaction between the two is a complicated one, which cannot be fully understood without accounting for both technical and social factors. While it might be harder to implement a decentralized system that is fully privacy-compliant, transparency and privacy should, however, not be regarded as being in a fundamental conflict. Quite to the contrary, the two are to a large extent compatible, and perhaps even complementary to a lesser extent.///////

Stephen Quilley, Jason Hawreliak, Kaitlin Kish

Finding an Alternate Route

Towards Open, Eco-cyclical, and Distributed Production

Open source networks have the potential to radically influence areas which have traditionally been under the purview of governmental and corporate entities. Traditional manufacturing, for instance, has often relied on institutions of scale for capital, distribution, and bureaucratic support. However, with the proliferation of open source networks, small, independent actors can collaborate with one another without relying on broad institutional support. This circumvention may potentially bring with it a number of economic, environmental, and psychological benefits. With these ideas in mind, and through drawing on exemplars such as Open Source Ecology, this paper explores the logic of the distributed, open architecture of a "reMaker society," focusing in particular on the problems of meaning and alternative modes for the provision of public goods. To unravel the connections between political economy, technology, and problems of meaning and behaviour, we propose the concept of the "reMaker society," which places value in community based manufacturing practices, localized distribution networks and shifts markers of social prestige from consumption to making.

KEYWORDS: *reMaker society, distributive economy, consumption, open source networks, immortality project*

INTRODUCTION

It is clear that solving the problems associated with globalization, feelings of alienation, and climate change will take more than technical and economic advances alone. For starters, it seems likely that part of the solution must come about by better understanding the role of consumer culture in bolstering self-esteem and ontological security (Laing, 1961; Giddens, 1991). Thus, one way to counter the logic of passive consumption may be to provide alternative sources of meaning and self-esteem – hero/immortality projects that privilege making and repurposing over buying and throwing away. This is a central aim of the reMaker society: not directly to replace or upend globalization and capitalist hegemony, but to offer a meaningful alternative to the logic of passive consumption. The concept of the reMaker society seeks to link the potential of open source technics, the DIY ethos, and maker-spaces, to an alternative vision of political economy and psychologically informed understanding of green hero/immortality projects.

EXPLORING A REMAKER DISTRIBUTIVE POLITICAL ECONOMY

In the global consumer economy, high turnover, inbuilt obsolescence, passive consumption and cycles of trivial innovation, short product life and disposability are difficult to disentangle from either welfare and more general social progress or the trajectory of technical innovation per se.

///This is because high rates of public and private investment depend upon fiscal transfers from an expanding economy. In this sense there is no trivial consumption. The reMaker society concept starts to unpick this Gordian knot in a number of ways.///

› **Open source design** *in the context of a community of makers would emphasize on modularity, repairabilty, upgradeablity and recyclability as design parameters. Removing the processes of design and fabrication if only partially from corporate cycles of investment and profit would allow the emergence of technologies with intrinsic design characteristics rather products imprinted by the extrinsic logic of the corporate ecosystem. The beginnings of such an ecosystem are discernible in OSE's system of open product releases and in the culture of Instructables, IkeaHack, Make Magazine and numerous open hard ware projects.*

› **Bioregional material flows** *and reduced global trade in products and raw materials would create an economic and design premium in favour of material recycling but also salvage, component recovery and re-use.*

› **Modular design** *would minimise wastage associated with repair, recycling and upgrading (as with start-up modular Phoneblok – 'a phone worth keeping'); maximise the coherence of product sets both in domestic and commercial settings – and so reduce the tendency towards the duplication of hardware (as with OSE's Global Village Construction Set).*

› **Reflexive local manufacture:** *The geographically dispersed but functionally integrated manufacturing systems operating in abstract space of the global economy are characterised by opaque and unreadable supply chains. The potential of a bioregional reMaker society would be to minimise the length and complexity of supply chains, to make visible the full financial, ecological, material and social costs of production and to make comprehensible the relationships between consumers and producers. From a systems perspective this reflexivity would enhance the feedback loops and information flows regulating processes of production.*

CONCLUSION

The reMaker society offers a number of possibilities for community structures centred on open source technics of relocalization. While still dependent on global production chains, the ongoing aspiration for relocalization is for the first time supported by technological innovations and micro-fabrication that give hope for a shift away from a corporately dominated political economy. Such a political economy, bolstered by growing support for open-source/commons ownerships and approaches would be more likely to achieve a 'sustainable degrowth' (Martínez-Alier, 2010) by a) making visible impacts on local bioregions and ecological systems and b) restructuring satisfaction toward a more limited set of needs. It would also redefine ownership, both of goods within a community and toward a single produced good.

///Citizens would be engaged, embedded in community and place, gaining satisfaction through family, community, and creative activities. ///

All of this sounds like the idyllic visions of a post-growth society. However, open production and the distributed economy make conceivable such social structures in conjunction with high-tech production and technological innovation. With satisfaction coming from community and kin ties, a potential post-consumer, yet high-tech, society becomes possible.

EXPERIMENTAL FORMAT

Melanie Dulong de Rosnay

Alternative Policies for Alternative Internets

Online services Terms of Use (ToU) or End-user licence agreements (EULA) are often unfair, abusive and hard to read for users. They are also difficult to draft for alternative projects willing to develop fair and clear policies for their contributors. This piece provides examples of original and alternative clauses, containing fair and unfair terms, addressing some of the most common issues faced by online platforms when developing their legal policies regarding ownership of user-generated content, protection of personal data, liability for third-party content, and other legal questions affecting users' or consumers' rights and their enforcement.

////This contribution is intended to provide a practical, critical and normative contribution by proposing guidelines for platform developers drafting terms of use. ////

My legal approach is grounded in commons-based peer production theory and practice from a continental European legal culture perspective, with the assumption alternative internets have political concerns for freedom, autonomy, consent, privacy, independence, surveillance, asymmetries of power, security, unfair contractual and commercial practices and other fundamental rights. Neither universal nor exhaustive, and rather than legal advise, the purpose is to raise awareness on the possibility to draft alternative terms of use, in a context dominated by US corporate legal culture aiming at maximising profit and minimising risks (Google, Amazon, Facebook and Apple). Instead of embracing a neoliberal agenda, alternative policies may rather try to support the development of sustainable services and products, seen ascommons.

//// Alternative platforms are in a position of embedding political choices when selecting and developing their techno-legal infrastructure.////

//// To certain degrees, they may or may not take ownership of the work developed by their contributors; they may or may not facilitate others to reuse or profit from it; they may or may not be collecting and further disclosing personal data, either voluntarily provided or left unintentionally by users; they may or may not offer warranties on their product or service. ////

//// Apple **"You agree that: (1) your submissionsand their contents will automatically become the property of Apple, without any compensation to you"////**

//// 500px **"you hereby irrevocably waive allmoral rights in your Store Images"////**

//// Spotify **"You grant perpetual license to anything you publish"////**

//// SoundCloud **"You only grant to SoundCloud the rights necessary to operate the services."////**

//// The Copyheart Manifesto **"♥ Copying is an act of love. Please copy and share."////**

//// Don't Ask Me About It License **"Copying and distribution of this file, with or without modification, are permitted in any medium provided you do not contact the author about the file or any problems you are having with the file. Do what you want, just don't contact the author."////**

//// PicoPeering Agreement v1.0 **"There is no guaranteed level of service"////**

//// Twitpic **"You agree to indemnify Twitpic and its employees from any claim made by any thirdparty related to your content. That includes paying reasonable attorneys' fees."////**

A FEW WORDS FROM OUR REVIEWERS

"Such assumptions of the technologically empowered community versus the state have to be critically interrogated rather than taken on board"

"The framework is very interesting and the examples of the 'revealing tensions' at the different layers are well provided."

"Isn't the goal of competition exactly to win by outmanoeuvring (i.e. eliminating, acquiring etc) competitors to maximise market power and control?"

"[This paper] stands as an inspiring argument for the relevance of the artist's role as "the facilitator, the mediator, the commoner of knowledge and experience".

"The Internet is also decentralized."

"The 'Digital Craftsman' is an unfortunate term choice. I'd suggest the term change to 'Digital Craftsperson', already accepted in major dictionaries."

"The risk of the protocol locking in users is just as high [in decentralized] as in centralized architectures, since only when a system is built with data export mechanisms is user lock-in prevented."

"Many of the examples rely on properties of open source software, rather than decentralized networks"

All reviews, signals, original (initial draft) and published versions of this issue's papers are available here:
http://peerproduction.net/issues/issue-9-alternative-internets/peer-reviewed-papers/

JOPP REVIEW PROCESS

http://peerproduction.net/peer-review/process/

Our approach to peer reviewing is informed by Whitworth and Friedman's (2009a) criticism of current academic publishing as a form of competitive economics in which "scarcity reflects demand, so high journal rejection rates become quality indicators". This self-reinforcing system where journals that reject more attract more results in a situation where "avoiding faults becomes more important than new ideas. Wrongly accepting a paper with a fault gives reputation consequences, while wrongly rejecting a useful paper leaves no evidence". Whitworth and Friedman (2009b) propose an alternative evaluation system:
1. higher rating discrimination: a many-point scale, not just accept-reject
2. more submissions to be rated: rate all
3. more people to rate: community involvement
4. different ways of rating: formal review vs. informal use ratings.

MAIN STEPS:

Once authors have completed a full submission, they send it to the editor who assigns it to three anonymous reviewers. The reviewers assess the paper following our suggested review categories (see Appendix A). Once the reviewers have provided any necessary recommendations for improvement, these reviews are sent to the author for possible revision and the author decides whether to follow these recommendations.

The revised paper is sent back to reviewers for final evaluation following signaling categories (see Appendix B). The editor forwards the signals to the author, who then decides whether to publish the paper or not.
The paper is published alongside the signals. Signals will remain anonymous to ensure frank and fearless signaling.

NOTE:

– All reviews will be released alongside published papers. Reviewers may opt whether to remain anonymous or not.
– All initial draft submissions will be released alongside published papers unless the author provides compelling reasons (such as privacy of author or subjects) why this should not be the case.

THE FULL PAPERS ARE AVAILABLE AT:
http://peerproduction.net/issues/issue-9-alternative-internets/

supported by

netCommons