Alison Powell

Hacking in the public interest: authority, legitimacy, means and ends

Article (Accepted version)
(Refereed)

Original citation:
Powell, Alison (2016) *Hacking in the public interest: authority, legitimacy, means and ends*. New Media and Society . pp. 1-17. ISSN 1461-4448
DOI: 10.1177/1461444816629470

Hacking in the Public Interest: Authority, Legitimacy, Means and Ends

Alison Powell
Assistant Professor
Department of Media and Communications
London School of Economics and Political Science
Houghton Street, London WC2A 2AE UK

Bio

Alison Powell is Assistant Professor in Media and Communications at the London School of Economics and Programme Director of the MSc in Media and Communication (Data & Society). Her research examines how people's values influence the way technology is built, and how discourses, practices and governance structures are produced in relation to new technological systems.

Abstract

The cultural appropriation of ideas about hacking and opening knowledge have had significant impact on ways of developing participation in creating knowledge in the public interest. In particular, the ideal of hacking as developed through studies of free and open source (F/OS) has highlighted the value of processes of participation, including participatory governance, in relation to the value of expanded accessibility of knowledge, including knowledge commons. Yet these means and ends are often conflated. This paper employs three examples of projects where hacker-inspired perspectives on scientific knowledge contend with institutional perspectives. Each example develops differently the relationships between means and ends in relation to contests of authority and legitimacy. The paper's analysis suggests that while hacker culture's focus on authority developed in relation to participation has had great traction in business and in public interest science, this may come at the cost of a potential contribution to rethinking the value of knowledge in the public interest.

Keywords

Hacking, open source, knowledge construction, authority, public interest, open science

Introduction

In trying to understand the cultural significance of hacking and DIY culture, it's easy to conflate means and ends. Much research on hacking has focused on how participatory engagement creates alternative ways of engaging with machines, intellectual property or material. At the same time, there is another interpretation threaded through scholarship on hacking – that it has ends, and that the hack might transform the way the machine works, the way knowledge is shared, or the material object's final form. This interpretation is especially salient for studies of hacking in the free software tradition and in discussions of the importance of creating knowledge commons using intellectual property hacks. Yet means and ends are rarely separated, even when hacking culture is explicitly connected with the notion of the public interest, as it is in relation to open knowledge and science. This paper pursues two (slightly contradictory) goals: 1. To advance an ethical critique of the focus on participation within hacking culture; and 2. To explore how this focus on participation conflates the means and ends of hacking practice. To draw out the first point, it builds upon Mansell's (2013) analysis of how modes of authority become significant for managing knowledge commons, examining the relationship between the legitimacy of participation within hacking culture and "adaptive" forms of authority. To develop the second, it extends Collins and Evan's (2002) discussion of expertise and public knowledge and reveals how a focus on authority and legitimacy in relation to participation (rather than engagement with other politics of expertise) prevent a true focus on what the outcomes of hacking might produce for expanded notions of the public interest.

To develop these two linked arguments, I consider three examples of projects where hacking culture is positioned as contributing to the public interest. In the first example, the development of the CERN Open Hardware License (CERN OHL), researchers in the Beams and the Knowledge Exchange Sections at the European High-Energy established an open-source community that deliberately included members whose authority emerged from their long association with either open source license development or the practice of open hardware development. In the second example, the non-profit PublicLab employs open hardware as part of a strategy for broadening environmental inquiry that is consciously linked to DIY ethics and what Ratto and Boler (2014) refer to as ‘critical making.’ In this mode, the DIY ethos is a ‘critical’ activity that ‘provides both the possibility to intervene substantively in systems of authority and power and that offers an important site for reflecting on how such power is constituted by infrastructures, institutions, communities and practices” (p. 1). In the third example of the Internet of Things Academy, more accessible hardware raises questions about what kinds of scientific data garners more legitimacy. Designers on this project employ hardware sensors including noise and air quality monitors, that produce well calibrated measurements of similar quality to those used by scientific professionals. All of the examples engage with the notion of open hardware, enrolling these projects in debates about the means and ends of hacker projects like the GPL (see Powell, 2012).

Open hardware raises questions about how to extend the provisions for keeping intellectual property in commons. This is similar to what Barron refers to as “the tendency to problematize the technical infrastructures underpinning today’s digitally mediated public spheres” (2013, p. 599). To practitioners seeking to maximize participation in technological or scientific knowledge production, open hardware puts equipment in the hands of ordinary people, permitting a hack of science itself (McQuillan, 2014). In addition, open hardware can contribute to a DIY ethic of creative repurposing that positions hacking, tinkering and making of scientific measurement equipment as political in itself. The examples in the paper illustrate how the contests of authority within hacking culture gain greater political significance when they are played out over concerns related to the public interest.

Hacking culture and its contests

Hacking and hackers have transformed the social world outside of software. Social researchers situate hacking as a form of spontaneous techno-cultural jouissance (Levy, 1984; Thomas, 2002; Jordan, 2008), as a model for participation-based governance (Mateo-Garcia and Steinmueller, 2008; Dafermos 2013; Kostidiakis 2013) with the possibility to transform markets more broadly (Benkler 2006; Benkler 2011), as the enactment of critiques of the politics of technological systems (Kelty, 2006; Barron, 2013; Bodo, 2014; Sauter, 2014) and intellectual property systems (Lessig, 2006; Barron, 2012), or as an engagement with the culture and performance of masculinity and expertise (Dunbar-Hester, 2011). We also assess the relationship between hacking and the social, political and economic systems that are transformed by expansions of hacking practice. When Wark (2013) writes that “the hacker makes something new out of property that belongs to everyone in the first place” (p.73) he, like Soderberg (2008), claims that hacking reveals as well as transforms cultural and technical products, making us aware of their status as common knowledge usable by all.

Here we are reminded that hacker participation in creating projects like free and open source software (F/OS) led to the development and transformation of political values like liberalism (Coleman, 2012) through development of 'recursive publics' who create the means for their own perpetuation (Kelty, 2006) and through the reworking of intellectual property regimes to suggest possibilities for the creation of knowledge in commons (Stallmann, 1989; Lessig, 2006). We are also reminded of the possibilities for 'democratic rationalization' of technology (Feenberg, 2008; Milberry 2014) and hence the possibility that hacking, as a form of DIY practice, could prefigure or perhaps exemplify a democratization of technical or scientific knowledge. These varying political outcomes also include the contention that participation in hacking and other DIY projects models a democratization of knowledge through 'critical making' (Ratto, 2011; Ratto and Boler, 2014) and a potential transformation and broadening of scientific publics through DIY speculation through design (Di Salvo, 2014).

At the same time, features of hacking culture can re-invigorate existing cultural formations, for example through the development of open-source organizational culture within F/OS and its subsequent embedding of participation-based value within software production economies (Weber, 2006; Berdou 2011), and 'prosumer' practices (Moody, 2002) leading to the development of different products (von Hippel, 2005). Also in the economic sphere, the participation and networked relationships have been claimed as foundations for a network and reputation-based economy (Benkler, 2006). This reading of hacking culture celebrates individualism, participation, and reputation within a 'new spirit' of capitalism (Barron, 2013) and neoliberal governance (Cammaerts, 2011).

In this review of hacking's significance, two strands emerge: one, a valorization of participation, both as a feature of governance and as a mode of engagement with institutional power; and two, a evocation of a transformation of knowledge production and accessibility, extending from technical to scientific knowledge. The two strands illustrate how hacking culture is associated with transformations in means (participation) and ends (most often, the modes of production of software, but now, the modes of production of scientific and public interest knowledge). These are often conflated. This paper intervenes in this debate to provide an analysis of the consequences of the focus on participation rather than outcomes of hacking. These consequences include the market appropriations of hacking processes already considered in the literature (Cammaerts, 2011; Powell, 2012) as well as a limited transformation of the processes of scientific and public interest knowledge production.

The paper builds on previous work on authority and legitimacy in relation to both participation and knowledge production in hacking culture, especially the principles of adaptive and constituted authority developed by Mansell (2013), and the assessment of how contests of legitimacy (Collins and Evans, 2011) relate to transformations in knowledge practices. This extends previous work on governance and participation within hacker communities (Kostakis, 2010; Kostakis et al 2014), particularly F/OS hackers (Dafermos, 2001; Dafermos and Soderberg 2013), but also follows a turn in the science studies literature on expertise that has become increasingly concerned with how expertise is legitimated in different contexts.

Authority and legitimacy: F/OS and the GPL

Hacking culture sets up novel dynamics of authority: hackers are understood to establish their own authority, or "knowledge of purpose and technique acquired and demonstrated through participation" (Steinmueller and Mateo-Garcia 2008 p. 336). In contrast to the authority associated with institutions accrued through symbolic reinforcement of the functional necessity for an institution (Castoriadis, 1987), the authority associated with hacker culture is rooted in the imagination of participation and in expertise consolidated through participation. Other scholars of hacking in the DIY vein have focused on how participation in building and rebuilding technology operate as strategies for eroding boundaries between experts and laypeople and redistributing authority (Dunbar-Hester, 2014).

These forms of authority and legitimacy have also supported existing institutions, especially the institution of market capitalism. Much work over the past decade has identified how hacking practices; especially those related to F/OS production contribute to expertise and economic production within firms (Weber, 2006; Mansell and Berdou, 2009; Tapscott and Williams, 2008). Barron notes that the valorization of individual participation that is part of F/OS production has significant risks for the notion of collective goods: "In a reputational economy, creative production becomes a means to the end of forging a publicly recognizable identity: the goal is not so much to produce a body of work that can take on an existence beyond oneself as to become an entrepreneur of one's self by associating as much activity as possible (preferably including that of others) with one's name. If unchecked, this will yield a culture in which (self-) promotion takes priority over production; it is also liable to obscure the collective effort that sustains every project, erode mutual trust and loyalty, and ultimately undermine the FOSS spirit itself" (2013, pp. 618). Barron identifies that the relationship between the means of authority developed through participation and the ends of production and collective value are collapsed and obscured by some features of the development of authority through participation. Other work goes further to examine the ambiguity of authority in relation to both participation and possible ways to develop (or value) knowledge. This second set of ideas raises questions about whether the emphasis on participation in hacking culture has consequences for its role in democratizing scientific knowledge production.

Contests of authority

In Mansell's (2013) analysis of how modes of authority become significant for managing knowledge commons, and in Collins and Evan's (2011) discussion of expertise and public knowledge, researchers identify how legitimacy develops through processes of participation which may not be matched in which ways they are perceived as being resolved.

Adaptive knowledge legitimated through participation

Mansell (2013) outlines how modes of authority become significant for managing knowledge commons, exploring the potential for collaborations between formal science professionals and loosely organized groups of people working on crowdsourcing projects. Differences in data curation highlight differences in the nature of authority - along a continuum between the 'constituted authority' of hierarchical relations established in reference to formal norms of science and its institutions, and the 'adaptive authority' "characterizing loose, bottom-up, often informal, forms of authority that are frequently associated with information activities of many loosely connected online groups" (2013 p. 256). Within these specific communities of practice, different individuals collect data that is valued differently depending on the form of authority the person's associated with. Constituted authority validates the participation of the individuals who are part of the crowd. Adaptive authority validates the quality of the data and its later utility within scientific practice. While the practices associated with adaptive authority valorize the aggregation and sifting of knowledge for immediate purpose (such as collecting information in online repositories), constituted authority is concerned with curation of 'useful' scientific information and validation of who gets access to that knowledge.

The notions of constituted and adaptive authority are helpful in developing a response to the challenge of creating 'open innovation' in scientific practice. In particular, Mansell's distinction between forms of authority highlights how scientific expertise remains associated with the valorization of certain forms of knowledge and control of their access. In scientific crowdsourcing, people outside of scientific institutions more often value knowledge for its immediate purpose, or for the reputational value that contributing might garner. This conflicts with forms of constituted authority that are more closely associated with 'expert' knowledge located within scientific institutions. The crowdsourcing dynamics that are the subject of Mansell's inquiry often create a power imbalance whereby "lay" contributors to crowdsourced scientific projects are positioned as amateurs and as data sources, rather than as collaborators.

This kind of contest between adaptive and constituted authority mirrors the kinds of contests usually associated with hacker culture, in which hacker ethics of critique and revelation are placed in contrast with ethics of enclosure.

Here, in addition to the contested politics of authority, two further dynamics emerge: a politics of expertise, which distinguishes expert and lay knowledge and which aligns with participation as the means of hacking culture, and a politics of commoning, which seeks to connect them through the development and management of knowledge commons – arguably the desirable ends for public interest hacking culture.

The politics of expertise

Collins and Evans (2013) highlight how expertise must be identified for political ends. They note that even within a framework where multiple forms of expertise are valuable, some gain greater legitimacy. There is one kind of expertise, often scientific, that "has gained a kind of universal authority across society in virtue of what everyone believes to be its efficacy" (pp. 251). In relation to this expertise others emerge, including a type of 'contributory expertise' that is in a field relevant to this highly legitimate expertise. Judgments then need to be made about the legitimacy of contributory expertise. Collins and Evans write, "it is more difficult to separate the credentialed scientist from the experienced practitioner than was once thought: when we move toward experience as a criterion of expertise the boundary around science softens, and the set of activities known as 'science' merges into expertise in general" (pp. 253)

In this context, what becomes important is not expertise but legitimacy. Legitimacy can be conferred through relationships to structures of authority but also – as all of the previous studies of hacking culture identify – through resistance to structures of authority. This hinge point between authority and legitimacy motivates interest in expanding access to an creation of scientific knowledge: as Collins and Evans point out, the high levels of legitimacy associated with 'core' scientific legitimacy lead to lower levels of certainty. This in turn means that other actors play roles in conferring legitimacy: the media, the people with 'contributory expertise', and other people in general. In this context, efforts to 'democratize science' in the public interest can be viewed as sites for the negotiation of legitimacy – the kind of sites we will shortly be discussing in relation to hacker culture and public interest science.

The democratization of scientific production is considered through research on 'open science'. The concerns of open science often have to do with the capacity to provide broader access to the literature, experimental materials, and data sharing (Wilbanks, 2007), or the capacity to integrate different types of information and knowledge as part of a broader innovation process (Lakhani and Panetta, 2007). These concerns foreground 'openness' related to accessibility, whether of code, data, or knowledge. This contrasts with the research on F/OSS (Coleman 2012) that places an emphasis on the process and politics of opening things up, where 'openness' connects with a politics of critique. They are also implicitly oriented towards participation as a value in itself rather than in orientation to an outcome, but this literature, more than the more canonical discussions of hacker culture's governance processes, also gestures towards the ideal outcome of the knowledge commons

The politics of commoning

The institutional arrangement of maintaining resources in commons has been thoroughly investigated by Ostrom (1990), and expanded through studies on various forms of commons data management (Fuster Morell, 2010) and open source software. Much previous work on the institutional management of such 'knowledge commons' has investigated forms of social ordering and governance (Madison et al 2014) generating important insights on how commons can be maintained. The commons has an orthogonal relationship to hacker culture. It is not necessarily always the end goal of hacking, in contrast to the expression of individual liberty that Coleman (2011) links to practices of F/OS activism. In the economic realm, a similar legitimacy linking participation to the 'spirit of capitalism' (Boltanski and Chiapello, 2005) has become integrated into 'lean' 'networked' modes of production. This, as Barron points out, "embed[s] new modalities of control over both production and consumption, and extend[s] commodification processes rather than curtailing them" (2013, p. 609). The question then becomes, as Mansell's work reiterates, whether the kinds of authority associated with 'contributory expertise' and networked participation of the kind valorized within hacking culture are able to transform other structures of power rather than being subsumed to them. F/OS production does create a commons of re-usable intellectual property, and the extension of this commons was one rationale for the development of open source hardware licenses (see Powell, 2012).

As an organizing and political principle, the commons challenges some of the separations between forms of expertise as outlined by Collins and Evans, and evokes the promise of hacking to enact disruption to release to the people something that always should have been liberated (to paraphrase Wark, 2006). The following section tracks how this promise has been enacted through different types of participation across three projects linked by their engagement with open hardware in relation to science and the public interest. They illustrate that contests of authority in relation to legitimacy often play out as confusions between the means and ends of 'hacking' knowledge systems.

Examples

CERN OHL

The first example, of the development of the CERN open hardware license, directly draws upon the notion of the knowledge commons as a means of integrating knowledge drawn from hacker and advocacy communities with knowledge produced within CERN. It also shows how hacker culture animates this integration, providing a way to highlight the flexibility and openness of a particular group of CERN researchers. The development of the CERN open hardware license thus fits within a longer history of knowledge exchange at the institute, but seeks a different kind of engagement with the 'non-expert' partners than some other projects.

Since it's founding in 1954, the European high-energy physics lab (CERN) has intentionally developed strategies for intensive scientific collaboration (Krige, 2001). The Centre is associated with what Collins (1998) has identified as 'open evidential culture'. CERN's most recent, complex and multidisciplinary work, the creation of the ATLAS particle detector and the development of the Large Hadron Collider, have also required intense collaboration employing distributed working processes that brought together culturally heterogeneous researchers working in very different institutional settings (Boisot, 2011). Boisot's description of the work on the ATLAS detector draws on a narrative familiar to scholars of F/OS and open collaboration, highlighting collaboration and 'emergent strategies' that Boisot frames as typical of adhocracy (Toffler, 1970). In his report, the flexibility of the membership's work was coordinated around the detector, solidified by shared values among the many participants, and facilitated by the use of ICTs. This narrative of flexibility and collaboration has been part of the institutional identity of CERN (see Collins 1998, Knorr Cetina, 1999), supporting the efforts to develop open hardware as a means to foster collaboration within and outside the institution. Although CERN uses crowdsourced science projects as one of their knowledge transfer strategies, the CERN OHL project is unique in that its public engagement comes mainly through the process of defining the parameters of the open source project

Javier Serrano of the Beams Section, and Myriam Ayass of the Knowledge Transfer section launched the project in 2011 as a way to standardize the intellectual property relations of submission to the repository for open hardware designs that Serrano had developed. In 2011, the two published a first version of the license and began consultation with hardware hackers and other open hardware advocates, visiting open hardware conferences and Maker Faires and establishing a public mailing list. The expertise and experience of the participants in these conferences and mailing list discussions was perceived as being essential for the development of the license.

The license was intended to provide a parallel for electronics designs to the GPL licensing that applies to all software code written at CERN. The GPL was chosen because "Open Source principles encourage the creation of open communities and collaborations of users invited to improve and complement the software and share their enhancements with the entire community. This accords with the historical CERN collaborative spirit and maximizes the in-kind return to CERN. In substance, this recommendation promotes the concept of collaborative dissemination . . . the Copyleft philosophy fits best with CERN scientific philosophy and tradition" (Fluckiger, 2012). The support within CERN for 'collaborative dissemination' foreshadows some of the challenges between balancing the means through which software is improved by greater numbers of participants, and the ends to which 'collaborative dissemination' might be directed.

In interviews with Serrano and with members of the Knowledge Exchange team, it is clear that the license was developed in order to facilitate collaboration with companies and with individual hackers and makers. But the interest was not only in ends, that is, in having a final product that would allow the Beams Section to work more closely with companies, or benefit from discussions among open source advocates. It was also about means, and the significance of employing a process that respected the expertise outside of CERN as much as inside. In this process, hardware hacker and advocacy communities were positioned as essential to the development of the open hardware license: "I see it sometimes as enlarging our team … because the documents are all public, if [a collaborator] happens to be from a company… he's just one more guy collaborating" (Javier Serrano, 2013, personal communication). Serrano describes himself as a facilitator but insists that he is not skilled enough to be a hacker: "I know impressive hackers, and I would not say I am in the same league as them. But I believe in teams a lot, and what I am doing allows them to do very cool stuff, so I'm very proud of that" (Javier Serrano, 2013, personal communication).

This vision is of an integrated team, where both the 'impressive hackers' located outside of CERN and the researchers within can work towards the same goal. In the CERN OHL project, the goal was to create a hardware license in the same mode as the GPL. This was for two reasons: Serrano was himself a free software advocate, and inspired by the notion of creating an ever expanding knowledge commons that would include hardware as well as software. His efforts to establish the CERN OHL contributed to an ecosystem of open hardware licenses that reflected different philosophical and political stances (see Powell, 2012). Gaining legitimacy and support from the open source advocacy community and from hardware hackers was essential for Serrano's broader goal of extending the GPL into new contexts.

To gain this legitimacy, the license was discussed on a mailing list. As Powell (2015) describes, these discussions demonstrated the difficulty of determining what open hardware referred to: accessible designs, plans whose components are totally re-usable, a better form of knowledge commons, or recipes and descriptions for construction placed in a repository. Contention between these different ways of thinking about open hardware was in part resolved by allowing the license to act as a 'boundary object' (Star and Greisemer, 1998) – a shared framework that permits collaboration between groups developing different kinds of knowledge.

The resolution of the mailing list discussion solidified the importance of adaptive knowledge and hacker relationships for the CERN OHL. As a result of points raised by the participants from the open source community, the license's new version included provisions that favoured this group's interests over those of the Beams Section and the Knowledge Exchange Section. The new version of the license removed a provision that would require anyone who used a licensed design to inform the person who licensed it about how they were using it. This would have been very helpful for CERN, since it would have allowed the Knowledge Exchange section to monitor the use of material and ideas developed within CERN. In short, this decision valorized the interests of the participants and aligned with their adaptive authority, rather than supporting the long-term interest of identifying where and how open-source material is produced. This was in some ways an action oriented towards the means of collaboration rather than the ends of better identifying open-source materials.

Not all members of the open source community supported the development of a GPL-type license for hardware as the best way to create and broaden a knowledge commons related to electronic designs. Longtime open source advocate Bruce Perens, one of the participants in the CERN OHL license development, and a well-known developer of open software licenses and standards argued that open hardware licenses have the unintended consequence of creating more, not less, focus on intellectual property. This grates against the hacker perspective on these issues. In an interview hosted on hacker site Slashdot, Perens writes:

> “There's an important thing we should be aware of about Open Hardware. It's backwards in a way. Richard Stallman's Free Software movement opposed software being copyrighted. Copyright does not, for the most part, apply to hardware designs because they are functional . . . Patents apply to hardware designs, but most Open Hardware designers never pursue a patent on their designs. What then do they license to others?
>
> It turns out that we have a group of people at CERN, and one of my favorite lawyers and Yahoo, and even me, trying to add restrictions to something that is, for the most part, already in the public domain. And it came to me that this was backwards, and that we could be working against our own interest that way…The problem is that when we start licensing things that are actually in the public domain, we create norms that the courts take seriously . . . If we were responsible for taking hardware designs from public domain to copyrighted status, we'd be shooting ourselves in the foot.” (Perens, 2014)

Perens is concerned that the efforts at resisting enclosure of intellectual property and continuing to allow space for critique of these frameworks is actually being limited by the move towards licensing. He’s concerned that focusing on means and valorizing adaptive authority might limit the positive consequences of hacking by rendering much knowledge inaccessible – a fundamental impediment to facilitating further re-use of common resources, and perhaps a brake on hacking practice.

The development of the CERN Open Hardware license, then, is a consolidation of a particular perspective on the extension of GPL-inspired legal frameworks. In the extensive discussions on the CERN-OHL mailing list analyzed in Powell (2015), the challenge of successfully extending the principles of the GPL so that they would fully apply to electronics did not quite overlap with the interest in employing GPL principles to either expand a knowledge commons or to monitor CERN's intellectual property. As Perens's critique highlights, participation in modifying the license, and valorization of that participation as an alternative to the authority of CERN, inadvertently valorizes a narrower interpretation of open hardware and may even have the consequence of limiting the expansion of open hardware as a form of commonly accessible knowledge. This example thus illustrates the long term consequences of valorizing participation for its own sake, and highlights the tensions between adaptive and constituted authority.

PublicLab

In the second example, the US nonprofit PublicLab also engages with ideas of open hardware and hacker cultural ethics, this time in relation to the democratic ethics of DIY. Public Lab, a non-profit organization based in the USA but with local projects running in locations around the world, develops and applies open-source tools to environmental exploration and investigation. With an explicit focus on democratization of scientific knowledge through making, the project came to prominence after it used homemade balloons and digital cameras to map the Gulf oil spill in 2010. It aims at breaking down inequities of knowledge production by supporting DIY methods of collecting scientific data: "DIY aims to make technology something anyone can develop; Public Lab aims to make scientific research in environmental issues something anyone can do well. To make something oneself is to have a sense of ownership of it, and we extend this sense to scientific tools and data" (Warren and Regalado, 2014, np).

Public Lab runs workshops around the world that teach people how to build relatively low-cost tools for environmental monitoring and community mapping, including kite-mounted digital cameras. Cindy Regalado, a London-based member of PublicLab, explains that these projects are intended to develop a ‘spark of interest’ among people, and to employ DIY methods to help them understand that they could make their own monitoring tools to use in any kind of project (personal communication, 2014). For PublicLab open source is understood as an ethic, linked to the DIY ethic of creative re-purposing of objects. The project aims to democratize scientific inquiry by democratizing the production of its measurement tools, but more specifically to expand the ability of people to feel capable of pursuing an interest or curiosity.

PublicLab’s interpretation of open source aligns with a different politics of expertise than the integration of ‘contributory expert’ authority to knowledge sharing at CERN. For PublicLab, the ethic of open source that motivates their projects is concerned with increasing accessibility of knowledge and allowing more people to understand how to collect and represent information about their lives and communities. In this enactment of public interest science, the public interest is served by the public understanding the principles of science and feeling empowered to participate. Although the project is best-known for supporting local residents in designing and deploying homemade aerial cameras to map the local impact of the Gulf oil spill, advocates stress that the purpose of these projects is not to develop tools that produce scientifically verifiable data, but rather to encourage participation in creating tools and understanding science.

This is especially evident in PLOTS, PublicLab's open knowledge repository, which includes research notes, designs and instructions on how to build scientific measurement tools, including aerial cameras assembled from inexpensive digital cameras and large home-made kites. While some electronics designs shared on PLOTS use the CERN open hardware license, the repository is mostly meant to allow people to openly share, create, and reproduce tools for measurement and story telling. The knowledge is 'open' because the equipment is relatively inexpensive and because know-how is shared through the research notes and instructions.

PLOTS valorizes adaptive knowledge. It focuses on the financial accessibility of materials and the significance of participation in using them and doesn't necessarily collect or share the results of that participation. It decenters scientific value away from sites of constituted knowledge and authority, which place more value on the quality of scientific results. PublicLab grounds knowledge in material practice – as their 2013 annual report reads, "creating tools and communities of expertise (whether local or scientific)" (PublicLab, 2014). While this has significant value as a way of valorizing alternatives to constituted authority, it also reinforces a divide between modes of authority; where scientific institutions are still sources of important knowledge, but not necessarily collaborators in the horizontal processes of co-creation. Furthermore, there is an important difference in how open hardware is imagined in the CERN OHL and in the PublicLabs contexts. In the former, open hardware refers to design specifications sufficient to allow the electronics to be constructed by someone with the appropriate skills, in the latter, to financial accessibility and ease of construction. These two different ways of conceiving of open hardware do align, as open source designs that can be re-used render hardware like the Arduino lower in cost and easier to use. But they also diverge. Attempts like the CERN OHL to develop a stock of re-usable hardware designs through the integration of hacker practices into scientific collaboration imagine open hardware differently than the Public Labs projects that valorize knowing through making.

As with the CERN case, there are complexities that highlight the differences in legitimacy in relation to means, and legitimacy in relation to ends. The DIY objects constructed in PublicLab projects help people without scientific knowledge to develop and amplify their comfort with scientific practice. However, this positions scientific knowledge and authority as something separate, rather than as something to be collectively developed. In terms of process, this means that the opportunities for consistent negotiation between forms of authority are more limited. In terms of result, the separation between forms of authority widens, and the legitimacy of institutional science is reinforced by the fact that the data collected by inexpensive sensors is often of poor quality or not comparable with data produced by scientific institutions. This distinction is at the heart of the separation that Mansell identifies between the two forms of authority. As she notes, this separation complicates efforts at establishing knowledge commons because of the conflict between different perspectives on which kinds of knowledge ought to be part of such commons. Finally, the explicit association between material engagement and empowerment, while central to the mobilization of hacking culture, also reveals the fractured relationships between technical prowess and other forms of empowerment related to race and gender (Dunbar-Hester, 2010). For PublicLab, shareable knowledge is not an end goal, but part of the process that is intimately linked to making and doing. All of the legitimacy is thus associated with means, rather than with ends that could include an ongoing scientific conversation or the production of scientific data.

Internet of Things Academy

The final example, the Internet of Things Academy (IoTA) run by the Superflux design agency, more accessible hardware raises questions about what kinds of scientific data garners more legitimacy. Designers on this project employ environmental sensors including noise and air quality monitors, that produce well calibrated measurements of similar quality to those used by scientific professionals including policy-makers. Data from these sensors are intended to challenge government data with data collected by citizens with particular concerns (aircraft noise and air quality). The quality of data (and thus of the hardware) becomes more important than their accessibility to the citizens.

IoTA has two pilot projects that use sensor based networks (the 'Internet of Things') to address civic concerns. These are designed so that engagement with the design of data collection and analysis is very accessible, while not insisting that participants must engage in construction of hardware. The IOTA project is meant to help to valorize things that citizens already know about, by employing sensor technologies along with 'little data' collection technologies like daily notebooks. The first pilot called NoiseNap, measured noise pollution under London flightpaths, and BuggyAir, a project currently under development, will distribute air quality sensors to families to mount on their baby buggies. These sensors will then measure air quality as it is experienced at ground level and in areas where children are travelling.

The BuggyAir project in particular encourages the development of very high quality data, according to Superflux founder Anab Jain. This is to encourage two possible outcomes: first, behavior change in participants and other individuals as a result of the BuggyAir readings (this might include avoiding walking on routes where the sensors record very high air pollution) and second, policy change on the part of governments and standards setters who might respond to legitimate high quality data. Jain explains: “Quality is important. How can you have accurate enough data so you can advocate for car companies to consider new standards for brakes [that are one of the major contributors to particulate matter (PM) ground level air pollution]. This is small data. It will never be big data, so it has to be good data” (Personal communication, 2015).

In contrast to the approach of PublicLab, where financial accessibility of hardware is a key feature of the project’s openness and accessibility, BuggyAir employs proprietary sensors that cost £500 each and which are precisely calibrated to have 97% accuracy in measuring air pollution of all types, including particulate matter which composes 80% of ground level air pollution in London. This calibration and quality are understood as increasing the legitimacy of citizen-collected data. Jain and her team are concerned that the very accessibility of inexpensive scientific tools may mean that the data they produce is not considered legitimate from the perspective of constituted authority: ‘these citizen science projects, they might have a button you can wear, but the data is not even 50% reliable” (personal communication, 2015).

The IoTA pilots stress the legitimacy of their sensor data as a pathway towards valorizing citizen perspectives. In the NoiseNap pilot the sensor data on noise levels is placed together with journal entries describing the context and experience of aircraft noise. However, in both pilots, the technologies of scientific measurement are black boxed. Thus, the projects valorize non-expert knowledge and the adaptive authority that investigates its social and economic context, but does so by closing off the material praxis of data collection.

In comparison to our other two examples, IoTA's engagement with hardware and public interest scientific knowledge is more oriented toward ends than means. The accessibility of hardware and electronics makes it possible to design civic data collection tools that use the same kinds of calibrations as the tools used by governments, but repositions the site of data collection so that communities whose interests may not be represented in official data collection can offer their data as part of their political voice. This constructs legitimacy in relation to constituted authority: the goal is to produce data that is valid on the terms that scientific and policy practitioners establish. The end goal of producing such valid data supersedes – to an extent – the means of participation that are the focus of other civic science projects.

Conclusion

DIY and hacking culture operate by undermining and appropriating systems and structures through material practice. This is more critique than integration, of institutional knowledge. The use of scientific hardware and measurement practices to collect and represent data coming from an alternative point of view illustrates some of the politics that can lie beneath engagements between adaptive and constituted authority. Producing, creating, curating and contextualizing data obtained through scientific equipment or using scientific methods may provide an entry into broader political or policy discussions. This is a departure from many of the ways that hacking culture has been connected with scientific knowledge and the public interest.

The examples developed in this paper illustrate how the development of legitimacy in relation to participation has often characterized the way hacking has engaged with institutionalized frameworks. Participation comes to be associated with forms of governance that are understood as valuable for market capitalism or even for the development of 'collaborative dissemination' in science. There are advantages of this: an ethic of participatory knowledge creation as developed through the CERN OHL, or a process of empowerment through appropriating science in a DIY ethic. But there are disadvantages too: that the development of the public interest, or the "FOSS ethic" is weakened by too much focus on 'adaptive' authority and participatory governance.

Possibly, too much of a focus on means as opposed to ends can limit the outcomes of this engagement. In other words, the means of participation can limit the ends of shareable knowledge creation. Is the solution to try to engage with science and policy on the terms that their 'constituted' authority establishes? What if this further mystifies science and technology, countering the efforts of DIY and hacking culture? As this paper illustrates, hacking culture evokes as an end goal the accessibility of knowledge, but its valorization of participation can many times limit the achievement of these ends. This is entangled with the ways that legitimacy is understood within hacking culture and within the scientific cultures that open-source projects now engage. Valorizing adaptive authority of participants strengthens the focus on means, rather than the end goals of scientific investigation, which are often underpinned by reference to constituted authorities like scientific institutions or policy makers. The analysis here suggests that hacking culture has indeed made a difference in ideas about how to produce open knowledge, but that the outcomes of that production have not always produced the radical openness that hackers (and others) seek.

References

Barron, A. (2012). Kant, copyright and communicative freedom. Law and Philosophy, 31(1), 1-48.

Barron, A (2013) Free software production as critical social practice, Economy and Society, 42(4), 597-625.

Benkler, Y (2011) *The Penguin and the Leviathan: How Cooperation Triumphs Over Self-Interest.* New York: Random House.

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

Benkler, Y. & Nissenbaum, H., 2006. Commons-Based Peer Production and Virtue. *Journal of Political Philosophy*, 14(4), pp.394–419.

Berdou, E (2011) *Organization in Open Source Communities: At the Crossroads of the Gift and Market Economies*. New York: Routledge.

Bodó, B (2014). Hacktivism 1-2-3: how privacy enhancing technologies change the face of anonymous hacktivism. *Internet Policy Review*, 3(4).
DOI: 10.14763/2014.4.340

Boisot M (2011) Generating knowledge in a connected world: The case of the ATLAS experiment at CERN. *Management Learning* 42(4) 447–457.

Boltanski, L. & Chiapello, E (2005 [1999]). *The new spirit of capitalism* (G. Elliott, Trans.). London: Verso.

Cammaerts, B (2011). Disruptive Sharing in a Digital Age: Rejecting Neoliberalism? *Continuum: Journal of Media and Cultural Studies*, 25(1), pp.47–62.

Castoriadis, C (1987 [1975]) *The Imaginary Institution of Society* (K. Blamely Trans.) Cambridge: Polity Press.

Coleman G (2012) *Coding Freedom: The Ethics and Aesthetics of Hacking*. New Haven, NJ: Princeton University Press.

Collins HM (1998) The Meaning of Data: Open and Closed Evidential Cultures in the Search for Gravitational Waves. *American Journal of Sociology* 104(2) pp. 293-338.

Collins, HM and R Evans (2002) The Third Wave of Science Studies: Studies of Expertise and Experience *Social Studies of Science* 32/2(April 2002) 235–296

Dafermos G (2001) Management and virtual decentralised networks: the Linux project. *First Monday* 6. Available at: http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1481/1396 (accessed Feb 20, 2015).

Dafermos G and Söderberg J (2009) The hacker movement as a continuation of labour struggle. Capital & Class 33: 53–73.

DiSalvo, C (2014) The Growbot Garden Project as DIY Speculation Through Design. In Ratto M and M Boler *DIY citizenship: Critical making and social media*. Cambridge, MA: MIT Press pp. 237-247.

Dunbar-Hester C (2010) Beyond "Dudecore"? Challenging Gendered and "Raced" Technologies through Media Activism. *Journal of Broadcasting & Electronic Media* 54: 121–135.

Dunbar-Hester, C (2014) Radical Inclusion? Locating accountability in technical DIY. In Ratto M and M Boler *DIY citizenship: Critical making and social media.* Cambridge, MA: MIT Press pp. 75-88.

Feenberg A (2008) *Questioning technology.* London: Routledge.

Fluckiger, F (2012) Final Report of the Open Source Software Licence Task Force. CERN. (Accessed September 8, 2014). http://cds.cern.ch/record/1482206?ln=en

Fuster Morell M (2010) Governance of online creation communities. Provision of infrastructure for the building of digital commons. Unpublished doctoral thesis, European University Institute, Florence.

Gunkel, D J (2005) Editorial: Introduction to hacking and hacktivism. *New Media & Society* 7(5) 595-597.

Jain, A (2014) Personal communication.

Jain, A (2015) Personal communication.

Jordan, T (2008) *Hacking: digital media and technological determinism.* Cambridge, UK: Polity.

Kostakis V (2010) Peer governance and Wikipedia: identifying and understanding the problems of Wikipedia's governance. *First Monday* 15. Available at: http://firstmonday.org/htbin/cgi-wrap/bin/ojs/index.php/fm/article/view/2613/2479 (accessed Feb 20, 2015).

Kostakis, V, Niaros V, Gioitisas, C. (2014) Production and governance in hackerspaces: A manifestation of Commons-based peer production in the physical realm?. *International Journal of Cultural Studies*. doi: 10.1177/1367877913519310.

Kelty, CM (2005) Geeks, Social Imaginaries, and Recursive Publics. *Cultural Anthropology*, 20(2), pp.185–214.

Kelty, CM (2008) *Two bits : the cultural significance of free software.* Durham, NC: Duke University Press

Knorr Cetina, K (1999) *Epistemic cultures: How the sciences make knowledge*. Cambridge, MA: Harvard University Press.

Krige J (2001) "Distrust and Discovery. The Case of the Heavy Bosons at CERN", Isis 92(3): 517-540.

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

Lakhani KR and JA Panetta (2007) The Principles of Distributed Innovation. *Innovations* (Summer 2007): 97-103.

Lessig, L., 2006. *Code and other Laws of Cyberspace (version 2.0)*, New York: Basic Books.

Levy, S., 1984. *Hackers*, Garden City, New York: Doubleday.

McQuillan, Dan. "The Countercultural Potential of Citizen Science." *M/C Journal* 17.6 (Dec. 2014). 23 Feb. 2015 <http://journal.media-culture.org.au/index.php/mcjournal/article/view/919>.

Madison, MJ, Strandburg, K, & Frischmann, B (2014). *Convening Cultural Commons.* Oxford: Oxford University Press.

Mansell R (2013) Employing digital crowdsourced information resources: managing the emerging information commons. *International Journal of the Commons*, 7 (2). 255-277.

Mansell R and E Berdou (2010) 'Political economy, the Internet and free/open source software development', in Allen, M, J. Hunsinger and L Klastrup (eds), *International handbook of Internet research*, Boston: Springer: 341-61.

Mateos-Garcia, J & Steinmueller, E (2008) 'The institutions of open source software: Examining the Debian community'. Information Economics and Policy 20: 333-344.

Milberry, K (2014) (Re)Making the Internet: Free Software and the Social Factory Hack. In Ratto and Boler *DIY citizenship: Critical making and social media.* Cambridge, MA: MIT Press, pp. 53-64.

Moody, G (2002) *Rebel Code: Inside Linux and the open source revolution*, New York: Basic Books.

Ostrom, E (1990) *Governing the commons: The evolution of institutions for collective action.* Cambridge, UK: Cambridge University Press.

Powell, A (2012) "Democratizing Production Through Open-Source Knowledge: From open software to open hardware" *Media, Culture and Society* 4*:* 691-708.

Powell, A (2015) "Open culture and innovation: integrating knowledge across boundaries" *Media, Culture & Society*, first published on February 5, 2015 doi:10.1177/0163443714567169

Perens B (2014) Interview: Ask Bruce Perens what you will. Slashdot. (Accessed September 8, 2014) Available at: http://interviews.slashdot.org/story/14/04/03/1350216/interview-ask-bruce-perens-what-you-will

PublicLab (2014) *PublicLab Annual Report 2013.*

Ratto M (2011) Critical Making: Conceptual and Material Studies in Technology and Social Life. *The Information Society* 27(4): 252-260.

Ratto M and M Boler (2014) *DIY citizenship: Critical making and social media.* Cambridge, MA: MIT Press.

Regalado, C (2014) Personal communication.

Sauter, M. (2013). "LOIC Will Tear Us Apart": The Impact of Tool Design and Media Portrayals in the Success of Activist DDOS Attacks. *American Behavioral Scientist*, *57*(7), 983–1007. doi:10.1177/0002764213479370

Serrano, J (2013) Personal communication.

Soderberg, J. (2008). Hacking capitalism: The free and open source software movement. London: Routledge.

Star, SL (2010). This is Not a Boundary Object: Reflections on the Origin of a Concept. *Science, technology, & Human Values* 35(5): 601-617.

Stallman, R (1999) 'The GNU Operating System and the Open Source revolution'. In Chris DiBona, Sam Ockman and Mark Stone (eds.) *Open Sources- Voices from the Open Source Revolution*, London: O'Reilly and Associates, pp. 53-70.

Superflux Design. (2014) IoTA: Internet-of-Things Academy, Phase 2. Available at: http://www.superflux.in/work/iota-phase2 (Accessed Feb 20, 2015)

Tapscott D and Williams A (2006) *Wikinomics: How Mass Collaboration Changes Everything*.New York: Portfolio

Toffler A (1970) Future Shock. New York: Bantam Books.

Thomas D (2002) *Hacker Culture*. Minneapolis: University of Minnesota Press.

Von Hippel, E., 2005. *Democratizing Innovation*, Cambridge, MA: MIT Press.

Wark M (2004) *A Hacker Manifesto*. Cambridge, MA: Harvard University Press.

Warren J and C Regalado (2014) Response to "How do DIY processes encourage citizen participation?" *PublicLab Research Notes* (Accessed Feb 20, 2015). http://publiclab.org/notes/Cindy_ExCites/06-25-2014/response-to-how-do-diy-processes-encourage-citizen-participation

Wilbanks J (2007) Cyberinfrastructure For Knowledge Sharing. *CTWatch Quarterly* 3(3) (accessed Feb 20, 2015) http://www.ctwatch.org/quarterly/articles/2007/08/cyberinfrastructure-for-knowledge-sharing/

Weber, S. (2004) The Success of Open Source. Harvard University Press.