**Technology Design and Power: Freedom and Control in Communication Networks**

Tamara Shepherd and Normand Landry

**Abstract**

The design of technologies with particular sets of affordances for user action reflects and embeds particular socio-political values in the technological artefacts themselves. In relation to networked communication technologies like the internet, design values of openness and decentralization accord with the hegemonic value of freedom as an inherently positive social and political concept. Yet freedom is also an elastic concept that contains the possibility for the freedom of powerful interests to exert controls – technological, state, and legal – over the very networks designed to facilitate freedom. This article reviews how such controls are made manifest, with a particular focus on the role of technology design, in the areas of surveillance, censorship, and intellectual property. It then concludes by addressing how such controls might be resisted using the affordances of open and decentralized networks. The interplay between freedom and control in communication networks is crucial for the construction of contemporary modes of citizenship, publics, and participation.

**Keywords**

technology, design, freedom, networks, control, resistance, citizenship

**Introduction**

The study of technology design from the point of view of values or ethics highlights how design builds particular affordances into technologies that both enable and constrain certain actions. In June 2013, for example, a story in the *Guardian* exposed the extent to which the Obama administration has mobilized social media and other networked platforms in a massive program of state-sanctioned surveillance.[[1]](#footnote-1) Through the program, code-named Prism, US government agencies the FBI and the NSA had been shown to be tapping directly into the servers of nine major internet companies, Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, and Apple, in order to retrieve a variety of personal information including audio, video, photographs, e-mails, documents and connection logs that enable analysts to track a person’s movements and contacts over time. In many instances, the internet companies that had designed their platforms to encourage a dispersed web of interpersonal communication actively cooperated with government demands for information by facilitating the FBI’s and NSA’s backdoor access to corporate servers.[[2]](#footnote-2)

The story of the Prism program shows how technologies resting on a network infrastructure that was designed to enable decentralized, open communication and freedom of expression also feature affordances that enable centralized control to take advantage of that fact, exploiting the popularity of networked platforms by using them to gain entry into people’s private lives. In addition to surveillance as a central dimension to network power dynamics, we might add the dimensions of censorship and intellectual property as forms of technological control. These three dimensions provide salient examples of how power works through design in often competing and contradictory ways, where intended values are shaped to some degree by technology designers, but then get appropriated by uses representing both ends of the political spectrum. This tension between freedom and control across both the design and implementation of communications technologies implicates competing values that in turn shape processes of public debate, participation, and citizenship. As we will argue, interests seeking to enforce greater mechanisms of control through contemporary networked technologies typically represent the government-corporate nexus of neoliberal political power, while alternative groups and individuals have attempted to reaffirm the decentralized and open characteristics embedded in the original design values of communications networks as networks of resistance.

**Technology design and power**

The base assumption of this paper holds that technology design is both the product of power relations – something, as Leonardi & Barley argue, that ‘arises out of conflict and negotiation among groups with diverse interests in the technology’s development’ (2010: 19) – as well as a strategic site of social and political struggle. Design is a mixture of knowledge, science, interests, power, capital and ideology, or ‘a function of interconnected social, cul­tural, technical, and economic factors’ (Flanagin *et al*. 2010: 180). Simply stated, ‘technology design’ can be seen as the ways that technological artefacts are shaped by programmers, engineers, and designers, working under the impact of market and governmental forces, in order to perform specific tasks. In this shaping, the technologies take on certain affordances that enable some uses and constrain others (Gibson 1977; Norman 1988), often in contradictory ways. Noble calls this the ‘double life’ of technology, ‘one,’ he says, ‘which conforms to the intentions of designers and interests of power and another which contradicts them – proceeding behind the backs of their architects to reveal unintended consequences and unanticipated possibilities’ (1984: 324-5).

To use the example of the internet, interoperability is a technical design feature that illustrates how values get invested in a particular technology. The internet’s technical design supports interoperability – which is the capacity for different systems to communicate with one another and exchange information – by following a standardized set of protocols for exchanging that information. The Transmission Control Protocol/Internet Protocol (TCP/IP) system is the network standard that combines packet switching at the connection-oriented layer (TCP) and at the internetworking layer (IP). A packet is a unit of information, which TCP/IP transmits as part of carrying out the functions of the internet’s most popular applications, such as the web, e-mail, peer-to-peer file sharing, and media streaming. Because TCP/IP offers reliable data transmission and is the network standard, it supports innovation that can make use of its relatively simple information transfer capacity within more complex applications. The interoperability facilitated by TCP/IP is intended to bolster innovation but not necessarily to direct the specific functions designed onto it: so for example, interoperability has made peer-to-peer file sharing possible, but also makes possible new forms of internet filtering. Interoperability thus facilitates innovation but also enables further control to be applied to the network through filtering and surveillance technologies, for example (Flanagin *et al*. 2010).

Similarly, the end-to-end structure of the internet both supports openness and decentralization, but leaves open the possibility for interference (Blumenthal & Clark 2001: 73). End-to-end means that while information travels through the network, as facilitated through interoperability that allows that information to be transferred across different platforms and systems, the application-specific functions that enable the information to be used and manipulated reside at the endpoints of the network rather that at intermediary points. So, for example, information does not get altered or transformed while it travels through the network – it can only be manipulated at its origin and destination. End-to-end thus enables information to be transferred more efficiently, since it is not being operated upon at intermediary nodes during transmission, and also supports a distributed network where only the end hosts need to process the information packets into their complete and correct form. The essential value embedded in the end-to-end design is network neutrality, where the network itself does not exert functions onto information as it travels. One key affordance of a neutral or ‘dumb’ network includes the decentralization of power (Lessig 2006: 111), but increasingly, interventions into this neutral network such as deep packet inspection – where packets of information can be examined (if not altered) in order to discern their contents – have allowed for the tracking of information and other online surveillance practices (Morozov 2011: 221). While these competing affordances show how internet technology can be shaped by its uses, they also show that those uses are partially envisioned by the designers of the network.

One of key values embedded in a decentralized vision for networked technology accords with a dominant social ideal of the late twentieth century: freedom. As Polanyi (1944) characterized the meaning of freedom in a complex society, the concept grows increasingly contradictory and fraught as it becomes more central to political justifications. He noted that while freedom has the connotation of being inherently good, its effects can also be negative for society at large, such as in ‘the freedom to exploit one’s fellows’ and ‘the freedom to keep technological inventions from being used for public benefit’ (Polanyi 1944: 164, 169). In Western countries, such as Canada and the United States, the notion of “freedom of the press” has been historically instrumentalized by private interests to support the consolidation of highly concentrated, convergent oligarchic media markets (Sénécal 1995; Bagdikian 2004; McChesney 2004) In this sense, ‘freedom’ serves as an elastic concept, one that can be mobilized for better and worse purposes. The role of freedom in the design of networked technologies attests to the value’s potential ambivalence: technology design may create certain affordances to protect freedom (of choice, or of expression, for example), which only end up compromising that freedom through enabling new forms of control. Thus, the impact of this version of freedom as a guiding design value is that open networks can serve as platforms for diverse interests, including, paradoxically, interests that seek to control those platforms and constrain the communicative freedoms of their users.

**Control in communication networks**

Lessig’s *Code, Version 2.0* (2006) is one of the key texts describing the relationship between values and the internet’s design, including how designed values of openness and flexibility are currently being threatened by various forms of control. Lessig details how the internet has grown increasingly regulable through changes to its design prompted by pragmatic commercial imperatives. These changes include increased identification rather than anonymity, which compromises many individuals’ rights to express themselves freely without persecution under situations like authoritarian regimes (Branscomb 1994: 1646). Identification typically gets enacted by cookies that track specific users’ behaviours online for marketing purposes. Commercially driven innovations in this area include the way that companies like Microsoft are working to build an ‘identity layer’ onto the web. Such a layer would consolidate existing tools for identification, such as the use of the security protocol in the Secure Sockets Layer (SSL) to protect connections to public sites, into an entire identity metasystem that would blanket all web activity.[[3]](#footnote-3) Moreover, greater ability to look into packets of information sent over TCP/IP protocol through deep packet inspection and filtering means that not only users’ identities, but the content of the networked data can be tracked, as in the Prism surveillance program. Finally, geolocation abilities enable a specific location of online activities to be pinpointed. Countering the values embedded in end-to-end design that promote network neutrality, these changes reflect values that are in the private, rather than public, interest, encouraging closedness and identification as opposed to openness and anonymity (Lessig 2006: 111, 71). This change in the values underlying internet architecture is crucial because code comes with certain affordances for user behaviour and by extension citizenship: ‘The code embeds certain values or makes certain values impossible’ (Lessig 2006: 125). As such, the book concludes that increasing regulation of internet through closed or proprietary code introduces detrimental levels of control that will not likely be curtailed by legal mechanisms, given a neoliberal political climate where the courts tend to interpret legislation conservatively in the interest of powerful corporate actors.

Working from Lessig’s account, we frame controls as those interventions into communications networks that are applied in order to restrict the range of their uses according to the interests of powerful authorities. These controls are of three main types:

1. Technological control, established upstream by manufacturers and software developers with the goal of limiting the functionality of technological devices to a range of desired uses;
2. Legal control, by the development or implementation of a regulatory regime criminalizing or penalizing deemed illegitimate uses of digital media technologies;
3. State control, by surveillance and monitoring, harassment and repression (Landry 2012).

These three types of control often intersect, as can be seen in the following set of dimensions that further illustrate what we identify as the role of technology design in controlling the uses of communication networks according to hegemonic neoliberal values.

**Dimension 1: Surveillance and security**

As outlined at the beginning of this article, surveillance through networked technologies is a major consequence of the proliferation of these technologies within all aspects of everyday life. Through tracking technologies on the internet and in specific web platforms like Google and Facebook, people both willingly and unknowingly share personal information that gets compiled into massive databases for both commercial uses, such as target marketing (Turow 2012), and governmental uses, such as homeland security (Regan 2004). The design of secure systems often involves using the network’s open architecture as a platform for surveillance in the name of enhanced security (Kroener & Neyland 2012; Nojeim 2010: 120). Surveillance practices work not only to access people’s information, but to sort and classify populations in order to manage them in a process called ‘social sorting’ (Lyon 2002). Social sorting denotes how, in being accessed through surveillance, information is used to classify populations – for instance, by gender, race, age, or other axes of identity. Technology ‘sieves and sorts for the purposes of assessment, of judgment’ (Lyon 2002: 20), and so works as a disciplinary measure that individualizes risk. Since the stated purpose of surveillance is to ensure security by pinpointing potential risks, social sorting achieves that by assigning risk values to individuals within a population – thus shoring up institutional power – mainly through the centralized processing of information that is cross-referenced among databases into a single, consolidated sorting system. The contribution of computing in this scenario can be summarized in its reinforcement of the social power of information; data can be transferred, stored, and reconfigured in ever more fast, enduring, and sophisticated ways: ‘Computer codes are thus extremely important for the ways that surveillance works. In a strong sense, surveillance systems are what are in the codes’ (Lyon 2002: 23). The codes, in turn, serve to redefine the meaning of contemporary citizenship in a society organized through endemic surveillance.

The result of new configurations of surveillance as social sorting is that internet technology has not necessarily facilitated the open space that techno-optimists may have envisioned (e.g., Lévy 2002; Toffler 1980; Negroponte 1995). Instead, it has supported the creation of a series of proprietary walled gardens, within which private interests have exercised unprecedented powers of surveillance and control (Lyon 2002). Particularly given the popularity of Web 2.0 technologies, where the disclosure of personal information is a necessary precondition for using the service, surveillance or ‘dataveillance’ practices form the central mechanism for profitability (Orito 2011). Facebook is a prototypical example of Web 2.0 dataveillance, where, rather than overseeing the movement of people’s bodies in physical space, surveillance systems oversee the movement of people’s personal information through networked technologies employed toward the economic goal of profit making. The challenges to citizenship posed by Facebook dataveillance in particular and Web 2.0 surveillance in general include: the complexity of the terms of use and privacy policies; digital inequality; lack of democracy; the commercialization of the networked communication; the advancement of market concentration; the attempted manipulation of needs through target marketing; the limitation of the freedom to choose, the unpaid value creation of users; and the lack of transparency (Fuchs 2011). When this kind of voluntary ‘personal mass dataveillance’ is added to the surveillance possibilities of computer networks in general, it highlights how design decisions can create a significant shift in social arrangements, public spaces, and participation. Perhaps more explicitly than anyone else, Facebook CEO and founder Mark Zuckerberg has linked design, value, and power in social media when he claimed that privacy is no longer “a social norm,” arguing that “people have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people” (Barnett 2010). The influence of design in this scenario is especially crucial when considering the fact that most users do not typically alter default settings. So even when there are available settings for increased privacy in the network, most users will not change them, leaving the defaults as ‘de facto regulation’:

[...] default settings about Web browser cookies and RFID chips will determine what personal information is shared by users and what is private. Similarly, default settings for filtering technology from Web browser content ratings to television’s V-Chip surely play a significant role in the overall flow of communications [...] This is another case where attention must be focused on default settings provided by manufacturers, or deference to third parties, co-regulation, or ‘individual freedom’ is really deference to software designers and a way of not talking about a technological and political decision with important consequences. (Shah & Sandvig 2008: 43).

The gatekeeping or regulatory function of defaults is significant not only with respect to privacy, but also in terms of internet freedom more broadly, where preset defaults can potentially restrict access to certain content or services. When information is thus protected within proprietary spaces, it becomes increasingly difficult for individuals to understand decision making processes that bear upon their rights as citizens.

**Dimension 2: Censorship and freedom of expression**

While networked technology offers more access to information and potential for freedom of expression with its end-to-end network structure, those freedoms are matched with new forms of control that enact new programs of censorship. Reflecting the inherent ambivalence of network freedom, this control through both design and legislation can subvert the initial openness of the network, but can also be countered by participatory design that preserves decentralization:

[...] free speech values – interactivity, mass participation, and the ability to modify and transform culture – must be protected through technological design and through administrative and legislative regulation of technology, as well as through the more traditional method of judicial creation and recognition of constitutional rights. Increasingly, freedom of speech will depend on the design of the technological infrastructure that supports the system of free expression and secures widespread democratic participation*.* (Balkin 2004: 6)

Free speech values can thus be protected or threatened through technology design, in concert with legal and regulatory frameworks. The potential benefits of internet technology for free speech include making the dissemination of ideas cheaper, making it easier to cross geographic and cultural borders, and making it simpler to modify information (Balkin 2004: 13; Fogelman 1999).

While, as Balkin notes, legal frameworks for regulation must enact measures to protect the freedom of populations, legislative action is not the only regulator of networked communication. As Lessig has famously characterized, ‘code is law’: meaning that code or the architecture of systems is the often unseen but salient regulator of how freedoms can be exercised (Lessig 2006). Since technology design embeds certain values by creating particular affordances for human action, ‘we can build, or architect, or *code* cyberspace to protect values that we believe are fundamental’ (Lessig 2006: 6, emphasis in original). In relation to freedom of speech online, UNESCO’s Division for Freedom of Expression, Democracy and Peace commissioned a report to examine the situation of free speech online since the first World Summit on the Information Society (WSIS). This report suggests that technological design is but the starting point for discussion of freedom of speech; larger changes happening in law and regulation are modifying the potential of the technology (Dutton *et al*. 2011; see also, Deibert *et al*. 2010; Zittrain 2008). Legal and regulatory provisions, such as those for protecting children or for harmful content, put online freedom at risk in three dimensions: obstacles to access; restrictions on user rights; and limitations on content (Dutton *et al*. 2011: 8). These policy considerations also come with new technological solutions for controlling freedom of expression online through a number of strategies including: age verification systems; content ratings; gatekeeping by cultural institutions (such as cultural and arts centres, museums, libraries, archives, information and documentation centres, etc.); filtering systems that look for blocked information rather than enacting the blocking themselves; and the moderating services of information professionals and providers (Culture Committee 2011: 5).

Controls such as filtering technologies – which determine what kinds of content can be delivered through a webpage, email or other means in what is essentially a form of automated censorship – are, in fact, enabled by the very openness of the internet’s technical protocols. The open standards that allow for interoperability between technologies support innovation in various forms, including innovation in online censorship technologies through privately developed filtering algorithms. The values embedded in filtering technologies – which counter the neutrality of information transfer and openness to various kinds of expression – show how proprietary interests, when left unchecked by government regulation, can shut down freedom of speech and operational transparency (DeNardis 2009). For instance, the increasing power of Google as a gatekeeper to online expression and information has ushered in new forms of censorship; Google has infamously facilitated state censorship in China through its search algorithms (Vaidhyanathan 2012). So, while regulation is needed to check private forms of censorship through proprietary standards, many of the international internet governance bodies are under political pressure to increase control for security programs with a stated aim to protect the value of freedom (Deibert 2012).

**Dimension 3: Intellectual property rights**

Intellectual property similarly finds its legal foundations in values of individualism, personal freedom and protection (both moral and material), and entrepreneurship. As an economic principle, it is associated with creation, innovation, and reward for risk-takers in an open, market-based society (Hilty 2012; Benhamou *et al*. 2012). It is a value aggressively advocated by a configuration of sets of interests – economic institutions and public representatives of advanced capitalist economies, lobbies of media producers and distributors, and technological manufacturers – who favour control over collaboration, security over openness, and personal accountability over collective appropriation. Intellectual property defines a particular kind of ‘thievery’ or ‘piracy’ – the illicit access, appropriation or distribution of non-rival goods without the consent of the rights holder. In other words, intellectual property rights implicate a process through which theft is not the deprivation of one’s property but the non-payment of a right of access or use for protected material (Benkler 2006: 38), and thus the concept of property can be seen to oppose other, more communal, values that might more effectively apply to non-rival goods.

For technology designers, both copyright and patents form the main intellectual property mechanisms for code, software, databases, and algorithms (Vaidhyanathan 2001: 153). These legal parameters, established in intellectual property legislation, have a direct bearing on the values embedded in networked technologies. While there has been a number of subsequent legislative moves around digital copyright worldwide,[[4]](#footnote-4) the most prominent example of this influence can still be seen around the impact of the US Digital Millennium Copyright Act (DMCA), the agenda-setting legislation passed in 1998 based on the World Intellectual Property Organization (WIPO) Copyright Treaty (Vaidhyanathan 2001: 160-3).

In one of its most controversial aspects, the DMCA reversed existing copyright law, where the ability to make copies for certain uses was protected by fair use and other uses were determined through the court system, by enabling companies to place digital locks on their content and then criminalizing any circumvention of those locks. The specific wording of the DMCA legislation’s anti-circumvention clause, which contains four main elements – a prohibition on circumventing digital locks; a ban on devices that circumvent digital locks; a ban on devices that circumvent copyright protection more generally; and a prohibition on the removal of copyright information – states: ‘No person shall circumvent a technological measure that effectively controls access to a work protected under this title’ (*DMCA*, Sec 1201.(a).(1)(A)). For technology design, this means that a ‘technological measure’ – digital locks – overrides the right to fair use. In other words, specific expressive practices – remix, mash-up, culture jamming to name a few – are anticipated and prevented with the support of the law, notwithstanding the legal and moral consideration accorded to the principle of freedom of expression, with which such practices are closely associated. The popular backlash to the DMCA’s restrictions might be seen to have conditioned the recent reforms to Canadian copyright law, where non-commercial remix practices as well as some small-scale circumventions of digital locks are allowed. Yet, the law retains a broad anti-circumvention provision that is among the most restrictive in the world, which evidences the impact of media conglomerates’ lobbying power throughout the lengthy process of copyright reform attempts in Canada since the early 2000s (Geist 2012). The story of the DMCA’s implementation and continued influence thus reflects a neoliberal imperative for policymakers to support private interests, most visibly due to the lobbying efforts of cultural industry associations, in the name of economic growth through technological progress (Gillespie 2007).

As the key component of contemporary copyright, the anti-circumvention provision highlights how technology design embeds particular values. In this case, the focus of the law has switched from the regulation of copying to the regulation of technological design by attempting to control copy-making at the level of the technology, using encryption (Gillespie 2007). The encryption of software or digital content using digital locks – also known as Digital Rights Management (DRM) – represents a technical implementation of the commercial imperative to thwart copying and sharing. But this technical ‘solution’ requires a whole political, economic, and cultural assemblage to support its functioning, for example, the legal provisions around the circumvention of digital locks. This assemblage shows how technology design functions as part of the broader infrastructure or ecology of networked communication. What the current configuration of this ecology has done to digital culture, including not only content industries but software and design industries, is to ‘seriously undermine fundamental public commitments to personal privacy and freedom of expression’ (Rimmer 2007: 171). This threat is especially widespread due to the nature of the internet’s design, where making copies – something that is now legally suspect – is in fact an automatic process in the TCP/IP packet switching protocol of the network (Vaidhyanthan 2001: 152). In this context, the pre-emptive function of digital locks punishes people before they have even engaged in directed piracy, by preventing them from copying at all, even when that copying is an automatic aspect of the network or when it is done for purposes protected under enshrined rights to fair use (Gillespie 2007: 255). As an extreme piece of legislation, the anti-circumvention provision shows how fundamental freedoms can be curtailed through a combination of design and legal mechanisms that serve powerful private interests.

In these three contexts – surveillance, censorship, and intellectual property – where private and government actors are aligned in the pursuit of increasing control over information networks, citizen interest in maintaining the positive, democratic values of freedom will need to be channelled into participatory technology design, along with activism that targets legal and state controls over technology.

**Resistance by design**

So far, we have outlined how technology design works among the technological, state, and legal controls affecting the expression of freedom in communications networks. These three forms of control are, in turn, resisted in three sites: in policy settings, where the rules shaping them are defined, debated and challenged; in the judicial sphere, where competitive norms that determine legal, acceptable and desirable uses of media technologies are weighed against each other; and in technology itself, in the code and hardware of devices. For each of these settings, the issue of access is crucial. This includes access to code and the tools needed to reconfigure technology (in order to facilitate subversion, resistance, and protest), access to venues where norms are defined and implemented (mostly legal institutions and courts), and access to the political settings where specific interests shape norms and define what is meant by the ‘public interest.’ Actions of resistance to the governance of media technologies can thus be framed in terms of their opposition to certain ‘formal as well as informal strategies, underpinned by particular political and economic interests, that shape the emergence of mechanisms designed to structure the direction of and behaviour in media environment’ (Freedman 2008: 23).

While, at some levels, the openness of the internet means that its infrastructure can be adapted for both democratic and repressive applications (Paré & Desbarats 1998), there are also certain core values embedded in that very openness. The fact that the internet affords openness points to these values, which are fundamentally democratic in that they reflect ideals of universality, free expression, and open access. Yet the expression of these values is modified by both legal and regulatory influences and further design developments (Spinello 2002). Feenberg has famously characterized this relationship in terms of modern rationality, where the pockets of ambivalence in technology design need to be explicitly addressed through democratic politics in design itself (Sikka 2011: 103). The main challenge to such democratization of design, also framed as an ‘ethical use of code’ (Spinello 2002: 232), is posed by the current political economy of media and communication systems. In a landscape where the design of networked technology and platforms is undertaken primarily as a function of late capitalist media conglomerates, ethical design tends to be overpowered by proprietary models that erode the internet’s capacity for democracy (McChesney 2013).

The asymmetrical power exerted over networks by private interests in late capitalism has been the focus of considerable work in critical communication studies (e.g., McChesney 2013; MacKinnon 2012; Morozov 2012; Castells 2009; Strangelove 2005; Spinello 2002; Lyon 2002). Reflecting early critiques of the culture industry by Critical Theorists, the internet under capitalism has been framed as an instrument that stifles critical thought, cultivates social anomie, and dulls individuals into seeking comfort and meaning through mindless consumption (McChesney 2013). Corporate power has been likened to authoritarianism (Morozov 2012), where regimes of ‘Facebookistan’ and ‘Googledom’ control their netizens through a kind of privatized political power (MacKinnon 2012). The story of companies like Google, Yahoo, Microsoft, and Facebook assisting the US government’s online surveillance program attests to this:

Internet companies around the world face mounting pressure from governments not just to block websites but to delete a wide range of content from the Internet completely, as well as track what their users are doing so they can be prosecuted or cut off if they do anything illegal. (MacKinnon 2012: 93)

In such a neoliberal configuration, the openness of the internet is compromised not only by controlling information flows, but by demarcating territorial boundaries onto the network according to state power (Spinello 2002: 2). The drawing of such boundaries threatens the democratic and participatory values embedded in open network technologies, and thus requires the dedication of designers – in addition to traditional policy activists – to maintain openness and protect internet freedom.

Designing systems expressly for democratic communication is a key component of stemming the negative effects of corporate and governmental control over the network. Free and open source software (F/OSS) communities have been exemplary in this regard, serving as a critique on proprietary regimes and an alternative to markets and hierarchy (Dizon 2010: 136). Through democratic principles of participation rather than governance, the F/OSS movement offers a resistant model for the design of technologies, the legal parameters of intellectual property, and even the use of technologies, as guided by values such as reciprocity, publicity, transparency, and accountability (Dizon, 2010: 139). The influence of F/OSS’s success can be seen in various projects for open and participatory system design, particularly with marginalized communities in the developing world (e.g., Fernández-Baldor *et al*. 2009; Srinivasan 2007). Empowering users to get involved in design processes, by making them more transparent and open for sharing, facilitates democratic system-building that is specific to local contexts and thus effective for enhancing community engagement (Srinivasan 2007: 724-5; Anderson & Bishop 2010), and also freedom (Fernández-Baldor *et al*. 2009: 19).

The process of designing as well as the system being designed both have a bearing on the democratic freedoms of specific communities. When these communities are expanded beyond the local to mobilize dispersed populations through Web 2.0 platforms, for example, the design of that participatory architecture is likewise influential on what kinds of freedoms can be enacted (Kavada 2009). While it is important to keep in mind that rather than determining people’s behaviour, design facilitates it through affordances (Kavada 2009: 38), network design still exerts considerable pressure on freedom and power (Benkler 2011). In the network, freedom means the degree to which entities in a given network can ‘influence their own behaviors, configurations, or outcomes (exercise freedom) and be immune to the efforts of others in the network to constrain them (be subject to their power)’ (Benkler 2011: 726). Given this definition of freedom as both agency and the absence of restrictions, philosopher de Sola Pool’s prescient book, *Technologies of Freedom* (1983), offers an apt vision of network freedom as simultaneously facilitated by the shape of decentralized networks and threatened by the constraints of capitalism and the nation-state.

While designing technologies for democracy works well as a ground-up strategy for implementing new communication systems in local and dispersed communities, most of the dominant network systems currently in use reflect the influence of increasingly privatized and centralized controls. In this climate, where designing entirely new systems is not necessarily feasible for those with marginal economic or political power, design has been used to subvert hegemonic control through hacktivism or ‘electronic civil disobedience’ (Gillespie 2007: 258). Tracing its roots to the same hacker culture that underlies the F/OSS movement, hacktivism involves using technical hacks to get around centralized system controls. For example, in relation to intellectual property rights, hacktivists have found ways to break encrypted locks on digital goods such as e-books (Postigo 2012). Through hacking, decryption, and manipulation of the code that defines DRM itself, hacktivism has, in many instances, allowed individuals to successfully re-appropriate the freedoms that have been stifled by copy-protection technology:

[...] the practice of designing and distributing technologies that may, for example, circumvent copy-protection measures or work around existing paradigms for content distribution can be carried out by individuals and is not limited to organizations (a point that in itself is significant). (Postigo 2012: 8)

Indeed, hacktivism offers individuals the power to disrupt system architectures, a power that is typically only accessible for larger organizations. Yet, when hacktivists do organize, their impact is potentially even greater, as in the case of a group like Anonymous, which has hacked major government and corporate websites in opposition to censorship and surveillance (Coleman 2011). Another example of organized hacktivism is Wikileaks, which has used hacking to access and publish secret government cables, making institutional politics transparent as part of democratic ideals of access to information (Benkler 2011).

The practices of hacktivism reflect not only its origins in the hacker ethos of early computer programmers, but also their contemporaries participating in 1960s and 70s civil protest movements in the US. The term electronic civil disobedience directly references this genealogy, where digital liberty is framed in relation to citizenship and human rights (Ziccardi 2012). In this formulation, technology design works as a tool to help people resist oppression, among other tools of liberation employed by activist groups, the scientific community, and spokespersons (Castells 2009: 321). The important feature of networked technology, among these other tools, is that it is largely accessible and efficient for political organizing: ‘every individual may become a part of a larger system that seeks to oppose the status quo, using the tools offered by the digital world’ (Ziccardi 2012: 81). Especially because the internet by its initial design is an open, end-to-end system, it offers the potential to subvert centralized systems set up by oppressive governments or capitalist scientific management (Strangelove 2005: 164-5; Dourish 2003; Galloway 2004). Yet, while the openness of the network enables internet technology to function as a tool for resistance, it requires an infrastructure of activism to direct collective organizing:

There are so many other factors, especially those grounded in the territory and in the human beings inhabiting it, that are considerably more decisive in guaranteeing the success or failure of actions of protest and civil disobedience. Technologies today can certainly be a facilitating factor in revolution, but only when guided by the hearts, brains, and concrete actions of the activists who put them to use. (Ziccardi 2013: 163)

**Conclusion: the work of freedom**

Any technology, not only the internet and contemporary communication networks, is situated within a specific time and place, reflects the ideas of its makers and its social context, and is applied according to diverse and conflicting interests. Yet it remains difficult to tease out the competing value systems that guide technological development, and not least because of the semantic plasticity of values as concepts that get defined, used, and appropriated in multiple and often incompatible ways. The fundamental ambivalence of freedom as a key value for technology design attests to this fact, where the effects of design intermingle with the effects of use to produce technological artefacts as fundamentally socio-technical. The internet’s original design as an end-to-end network that decentralizes control over the transfer of information, for example, embeds the values of openness, flexibility, and generalizability, but in so doing, leaves the possibility or freedom for powerful interests to exert various forms of control over the network. So while technology design serves to shape the possibilities of democratic communication over network infrastructure, it does not do so without competing interests in design values.

The practice of designing is thus an exercise in power, where design as a political process both resists and reproduces existing power relations. Governments’ and corporations’ influence over design practices and design values, when accompanied by an attendant lack of public transparency, threatens to erode democratic freedoms, ideals of citizenship, and human rights by exploiting the openness of the internet’s architecture. Paradoxically, it is the very openness of that architecture that affords the design and implementation of new forms of control, just as it affords new forms of resistance. This article has looked at values in technology design – especially the value of freedom – in relation to democratic communication, surveying the forms of control and resistance at play in areas such as surveillance, censorship, and intellectual property. While each of these areas illustrates the interplay between government, industry, and public interests at stake in the design of technological systems, it also shows an overall trend toward increased control and centralization of networks and code. Avenues for resisting this increased control through design include designing systems for participatory democracy, and using them for hacktivism or electronic civil disobedience. These avenues for resistance, along with more traditional activism in areas such as legal and policy reform, are important to study further in order to stem the threats to democratic freedoms posed by the tightening of information control. As such, we conclude with the proposal that ethical or values-based work in technology design critically interrogate affordances not just from a user perspective but from a broader social and citizenship perspective. Amid ever more pervasive systems for control, it is urgent that we reconsider the values underlying our seemingly neutral everyday communications technologies.

**Authors**

**Tamara Shepherd** (PhD, Concordia University) is a Postdoctoral Fellow in Information Technology Management at Ryerson University. Her work has been published in the *Global Media Journal*, *Canadian Journal of Communication*, and *Triple C: Communication, Capitalism and Critique*. Contact: 350 Victoria St., Toronto, ON, Canada M5B 2K3, tamara.shepherd@ryerson.ca

**Normand Landry** (PhD, McGill University) is a Professor at the Université du Québec a Montréal-Téluq and a researcher with the Groupe de recherche interdisciplinaire sur la communication, l'information et la société (GRICIS). He is the author of *Droits et enjeux de la communication* (2013) and *SLAPP: bâillonnement et répression judiciaire du discours politique* (2012). Contact: 5800 rue Saint-Denis, Bureau 1105, Montréal, QC, Canada H2S 3L5, normand.landry@teluq.ca

**References**

Anderson, L. and Bishop, P. (2010), ‘Communicative Mechanisms of Governance: E-democracy and the Architecture of the Public Sphere’, in R. Cropf and W.S. Krummenacher, (eds.), *Information Communication Technologies and the Virtual Public Sphere: Impacts of Network Structures on Civil Society*. Hershey, PA: IGI Global, pp. 52–71.

Bagdikian, B.H. (2004), *The new media monopoly.* Boston: Beacon Press.

Balkin, J. (2004), ‘Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society’, *New York University Law Review*, 79: 1, pp. 1–58.

Barnett, E. (2010), ‘Facebook’s Mark Zuckerberg says privacy is no longer a “social norm”’, *The Telegraph*, 11 January, http://www.telegraph.co.uk/technology/facebook/6966628/Facebooks-Mark-Zuckerberg-says-privacy-is-no-longer-a-social-norm.html. Accessed 19 June 2013.

Benhamou, F., Moureau, N., & Peltier, S. (2012), ‘La longue marche vers une appropriation

cognitive du web : le cas de la bande dessinée’, *Réseaux* 175: 5, pp. 83–105.

Benkler, Y. (2011), ‘Networks of Power, Degrees of Freedom’, *International Journal of Communication* 5, pp. 721–755.

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

Berners-Lee, T. (2006), ‘Neutrality of the Net’, http://dig.csail.mit.edu/breadcrumbs/node/132. Accessed 19 April 2013.

Blumenthal, M.S. and Clark, D.D. (2001), ‘Rethinking the design of the Internet: The End-to-End Arguments versus the Brave New World’, *Transactions on Internet Technology* 1: 1, pp. 70–109.

Branscomb, A.W. (1994), ‘Anonymity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspaces’, *Yale Law Journal* 104, pp. 1639–1675.

Castells, M. (2009), *Communication Power*. Oxford: Oxford University Press.

Coleman, G. (2011), ‘Anonymous: From the Lulz to Collective Action’, *The New Everyday: A Media Commons Project* 6, http://mediacommons.futureofthebook.org/tne/pieces/anonymous-lulz-collective-action. Accessed 23 April 2013.

Culture Committee, Conseil de l'Europe. (2001), *Public Access and Freedom of Expression in Networked Information: Guidelines for a European Cultural Policy*. Strasbourg, France: Council of Europe.

Deibert, R. (2012), ‘International Mechanisms of Cyberspace Controls’, in L. Diamond and M.F. Plattner, (eds.), *Liberation Technology: Social Media and the Struggle for Democracy*. Baltimore: John Hopkins University Press, pp. 33–46.

Deibert, R.J., Palfrey, J.G., Rohozinski, R. and Zittrain, J. (2010), *Access Controlled: the Shaping of Power, Rights, and Rule in Cyberspace*. Cambridge, MA: MIT Press.

DeNardis, L. (2009), ‘Open Standards and Global Politics’, *International Journal of Communications Law & Policy* 13, pp. 168–184.

De Sola Pool, I. (1983), *Technologies of Freedom*. Cambridge, MA: Harvard University Press.

*Digital Millennium Copyright Act* (*DMCA*). (1998), Pub. L. 105-304, 112 Stat. 2860.

Dizon, M.A.C. (2010), ‘Free and Open Source Software Communities, Democracy and ICT Law and Policy’, *International Journal of Law and Information Technology* 18: 2, pp. 127–141.

Dourish, P. (2003), ‘The Appropriation of Interactive Technologies: Some Lessons from Placeless Documents’, *Computer-Supported Cooperative Work* 12: 4, pp. 465–490.

Dutton, W.H., Dopatka, A., Hills, M., Law, G. and Nash, V. (2011), *Freedom of Connection, Freedom of Expression: The Changing Legal and Regulatory Ecology Shaping the Internet*. Paris: UNESCO.

Fernández-Baldor, Á., Hueso, A. and Boni, A. (2009), ‘Technologies for Freedom: Collective Agency-oriented Technology for Development Processes’, *Annual Conference of the Human Development and Capability Association*, Pontifical University of Peru, Lima, September.

Flanagin, A.J., Flanagin, C. and Flanagin, J. (2010), ‘Technical Code and the Social Construction of the Internet’, *New Media & Society* 12: 2, pp. 179–196.

Fogelman, M.L. (1999), *A Study of Freedom of Expression and Technology: The Case of Computer-mediated Communication (CMC)*. Albany: SUNY Press.

Freedman, D. (2008), *Theorizing Media Policy.* Paper presented at the Media, Communication and Humanity Conference, London, 21-23 September.

Fuchs, C. (2011), ‘New Media, Web 2.0 and Surveillance’, *Sociology compass* 5: 2, pp. 134–147.

Galloway, A.R. (2004), *Protocol: How Control Exists after Decentralization*. Cambridge, MA: MIT Press.

Geist, M. (2012), ‘What the New Copyright Law Means for You’, The Toronto Star, 10 November, http://www.thestar.com/business/2012/11/10/what\_the\_new\_copyright\_law\_means\_for\_you\_geist.html#comments. Accessed 12 June 2013.

Gibson, J. (1977), ‘The Theory of Affordances’, in R. Shaw and J. Bransford, (eds*.*), *Perceiving, Acting, and Knowing: Toward an Ecological Psychology*. Hillsdale, NJ: Lawrence Erlbaum, pp. 62–82.

Gillespie, T. (2007), *Wired Shut: Copyright and the Shape of Digital Culture*. Cambridge, MA: MIT Press.

Hilty, R. M. (2011), ‘La Constitution économique européenne et la propriété intellectuelle’, *Revue internationale de droit économique*, t.XXV(4), pp. 481–510.

Hugenholtz, P. B. and Okediji, R. (2012), ‘Conceiving an International Instrument on Limitations and Exceptions to Copyright’, Amsterdam Law School Research Paper No. 2012-43; Institute for Information Law Research Paper No. 2012-37, pp. 1–57.

Kavada, A. (2009), ‘Collective Action and the Social Web: Comparing the Architecture of Avaaz.org and Openesf.net’, in N. Carpentier, (ed.), *Communicative approaches to politics and ethics in Europe*. Estonia: Tartu University Press, pp. 129–140.

Kroener, I. and Neyland, D. (2012), ‘New Technologies, Security and Surveillance’, in K. Ball, K. Haggerty and D. Lyon, (eds.), *Routledge Handbook of Surveillance Studies*. London: Routledge, pp. 141–148.

Landry, N. (2012), ‘*Mouvements sociaux, technologies médiatiques et pouvoir*’, in S. Proulx, M. Millette and L. Heaton, (eds.), *Penser les médias sociaux. Enjeux pour la communication*. Québec : Presses de l'Université du Québec. pp. 153–169.

Leonardi, P.M. and Barley, S.R. (2010) ‘What’s Under Construction here? Social Action, Materiality, and Power in Constructivist Studies of Technology and Organizing’, *The Academy of Management Annals* 4: 1, pp. 1–51.

Lemley, M.A. (1997), ‘The Economics of Improvement in Intellectual Property Law’, *Texas Law Review* 75: 4, pp. 873–906.

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

Lévy, P. (2002), *Cyberdémocratie : essai de philosophie politique*. Paris : O. Jacob.

Lyon, D. (ed) (2002), *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*. London: Routledge.

MacKinnon, R. (2012), *Consent of the Networked: The Worldwide Struggle for Internet Freedom*. New York: Basic Books.

McChesney, R.W. (2013), *Digital Disconnect: How Capitalism is Turning the Internet against Democracy*. New York: The New Press.

McChesney, R.W. (ed) (2004), *Our Unfree Press: 100 Years of Radical Media Criticism.* New York: New Press.

McChesney, R.W. and Nichols, J.D. (2010), *The Death and Life of American Journalism*. Philadelphia: Nation Books.

Morozov, E. (2012), *The Net Delusion: The Dark Side of Internet Freedom*. New York: PublicAffairs.

Negroponte, N. (1995), *Being Digital*. New York: Knopf.

Nojeim, G.T. (2010), ‘Cybersecurity and Freedom on the Internet’, *Journal of National Security Law & Policy* 4, pp. 119–138.

Norman, D. (1988), *The Psychology of Everyday Things*. New York: Basic Books.

Orito, Y. (2011), ‘The Counter-control Revolution: “Silent Control” of Individuals through Dataveillance Systems’, *Journal of Information, Communication and Ethics in Society* 9: 1, pp. 5–19.

Paré, M. and Desbarats, P. (1998), *Freedom of Expression and New Information Technologies*. Québec: IQ Collectif.

Polanyi, K. (1944 [2001]), *The Great Transformation: The Political and Economic Origins of Our Time*, Second Edition. Boston: Beacon Press.

Portela, I.M. and Cruz-Cunha, M.M. (2010), *Information Communication Technology Law, Protection and Access Rights: Global Approaches and Issues*. Hershey, PA: IGI Global.

Postigo, H. (2012), *The Digital Rights Movement: The Role of Technology in Subverting Digital Copyright*. Cambridge, MA: MIT Press.

Regan, P.M. (2004), ‘Old Issues, New Context: Privacy, Information Collection, and Homeland Security’, *Government Information Quarterly* 21: 4, pp. 481–497.

Rimmer, M. (2007), *Digital Copyright and the Consumer Revolution: Hands off my iPod*. Northampton, MA: Edward Elgar.

Sénécal, M. (1995), *L'espace médiatique : les communications à l'épreuve de la démocratie*. Montréal : Liber.

Shah, R.C. and Sandvig, C. (2008), ‘Defaults as De Facto Regulation: The Case of Wireless Access Points’, *Information, Communication, and Society* 11: 1, pp. 25–46.

Sikka, T. (2011), ‘Technology, Communication, and Society: From Heidegger and Habermas to Feenberg’, *The Review of Communication* 11: 2, pp. 93–106.

Spinello, R.A. (2002), *Regulating Cyberspace: The Policies and Technologies of Control*. Westport, CT: Greenwood Publishing Group.

Srinivasan, R. (2007), ‘Ethnomethodological Architectures: Information Systems Driven by Cultural and Community Visions’, *Journal of the American Society for Information Science and Technology* 58, pp. 723–733.

Strangelove, M. (2005), *The Empire of Mind: Digital Piracy and the Anti-capitalist Movement*. Toronto: University of Toronto Press.

Toffler, A. (1980), *The Third Wave*. New York: Morrow.

Turow, J. (2012), *The Daily You: How the Advertising Industry is Defining your Identity and your Worth.* New Haven, CT: Yale University Press.

Vaidhyanathan, S. (2001), *Copyrights and Copywrongs: The Rise of Intellectual Property and how it Threatens Creativity*. New York: New York University Press.

Winner, L. (1980), ‘Do artifacts have politics?’ *Daedalus* 109: 1, pp. 121–136.

Ziccardi, G. (2012), *Resistance, Liberation Technology and Human Rights in the Digital Age*. London: Springer.

Zittrain, J. (2008), *The future of the Internet and how to stop it*. New Haven: Yale University Press.

1. The *Guardian* broke the story of the Prism program in June 2013 based on the classified documents provided by whistleblower Edward Snowden, former CIA employee; see: http://www.guardian.co.uk/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance;

   http://www.guardian.co.uk/world/2013/jun/06/nsa-phone-records-verizon-court-order;

   http://www.guardian.co.uk/world/2013/jun/10/nsa-spying-scandal-what-we-have-learned;

   http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data. [↑](#footnote-ref-1)
2. The *Guardian*, 2013; also see: *The Economist*, http://www.economist.com/news/leaders/21579455-governments-first-job-protect-its-citizens-should-be-based-informed-consent, and http://www.economist.com/news/briefing/21579473-americas-national-security-agency-collects-more-information-most-people-thought-will); the *Washington Post*, http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/ [↑](#footnote-ref-2)
3. See http://msdn.microsoft.com/en-us/library/ms996456.aspx for Microsoft’s proposal to build such an identity metasystem: ‘the role of an identity metasystem is to provide a reliable way to establish who is connecting with what—anywhere on the Internet.’ [↑](#footnote-ref-3)
4. For a review of these, see Postigo 2012; Hugenholtz & Okediji 2012. [↑](#footnote-ref-4)