RESTRICTING DIGITAL SITES OF DISSENT: COMMERCIAL SOCIAL MEDIA AND FREE EXPRESSION

Abstract

The widespread use of commercial social media platforms by protesters and activists has enhanced protest mobilisation and reporting but it has placed social media providers in the intermediary role as facilitators of dissent and has thereby created new challenges. Companies like Google and Facebook are increasingly restricting content that is published on or distributed through their platforms; they have been subject to obstruction by governments; and their services have been at the core of large-scale data collection and surveillance. This article analyses and categorises forms of infrastructure-based restrictions on free expression and dissent. It shows how private intermediaries have been incorporated into state-led content policies; how they set their own standards for legitimate online communication and intervene accordingly; and how state-based actions and commercial self-regulation intersect in the specific area of online surveillance. Based on a broad review of cases, it situates the role of social media in the wider trend of the privatisation of communications policy and the complex interplay between state-based regulation and commercial rule-making.

Keywords: Social media, Protest, Censorship, Surveillance, Digital rights, Freedom of expression

Introduction

Communication platforms and alternative media have been crucial sites for protest mobilisations, activist discourses, the creation of (counter) public spheres and the distribution of dissident information. From leaflets to the alternative press, from community radio to video activism, and from Indymedia to Facebook, communication sites have provided key infrastructure and have even defined protest and dissent - from Samizdat to 'sms protests' to 'Twitter revolutions'.

However, whereas many earlier movements tried to create their own media infrastructure, the most recent protest cycle has been characterised by the widespread use of commercial platforms. This has allowed broader publics to be involved in alternative discourses, but it has also created new challenges and restrictions as it has, for example, given commercial social media providers a role in both facilitating and limiting dissent. While companies such as Facebook and Twitter have actively supported the use of their platforms by protesters during the Arab Spring and similar uprisings, they have increasingly intervened in what can be published and have shaped the uses of their sites. This has been due, at least in part, to state pressures that restrict and monitor social media, and a regulatory trend that focuses on social media's role as key nodes in communication networks. In addition, Internet companies are developing their own rules that limit the range of acceptable content, services, clients and behaviours in accordance with their commercial goals.

This article will analyse new types of limitation placed on free expression and alternative discourses, restrictions that originate in a form of infrastructure that is now used predominantly for dissident communication. It will focus on the increasingly common practice of social media companies in censoring content and monitoring activists, and it will address them from the

perspectives of both external interventions by the state and the internal logics of commercial social media platforms. In addition to the challenges this poses to mediated dissent, as I will argue, the role of social media companies demonstrates a shift in governance that assigns private intermediaries a greater role in both implementing and formulating rules and regulations. It points to emerging policy-making arrangements where public and private actors intersect in the regulation of freedom of expression.

I will start by discussing social media as enablers of both dissident discourses and state control, and root this dichotomy in the social and economic logics of social media. The following three sections will address different dimensions of social media control. Through a range of examples, they will outline how private intermediaries are incorporated into state-led content policies; how they set their own standards for legitimate online communication and intervene accordingly; and how state-based actions and commercial self-regulation intersect in the specific area of online surveillance. Based on this broad review of cases, I will situate the role of social media in the wider trend of a privatisation of communications policy and a complex interplay between state-based regulation and commercial rule-making.

This article is based on research into social media trends and a wide review of current media reporting on social media activities and transformations. Furthermore, it draws from interviews and document analysis conducted as part of three collaborative research projects that are ongoing at the time of writing: ‘Digital Citizenship and Surveillance Society: UK State-Media-Citizen Relations After the Snowden Leaks’; ‘Mapping Global Media Policy’; and ‘Managing ‘Threats’: Uses of Social Media for Policing Domestic Extremism and Disorder in the UK’. Combining these different sources, it explores a variety of material to detail contemporary trends in the restriction of dissent on social media platforms.

The Two Faces of Social Media

From Indymedia to Twitter, social media and other interactive digital platforms have been an important means of activist and dissident communication, and have been used to spread alternative information and to organise and mobilise. The Indymedia network which emerged in 1999 and expanded around the globe over the following years pioneered citizen journalism by bringing alternative news to a global audience and by allowing every Internet user to publish their stories via its open publishing system and thus to contribute to a user-generated news platform (Hintz, 2014). The rise of blogging as a mass phenomenon and the widespread practice of 'citizen witnessing' (Allan, 2013) of key news events followed in its wake with citizen reports, pictures and audiovisual footage complementing and transforming traditional journalistic practices.

From the SMS protests in Spain and the Philippines in the early 2000s to the alleged 'Twitter'- and 'Facebook-Revolutions' in Iran in 2009 and Egypt in 2011, and to the more recent activities of the Yo Soy 123 movement in Mexico, the Gezi Park protests in Turkey, or the Umbrella movement in Hongkong, social media have been widely credited as an important force in supporting social and political change (Dencik and Leistert, 2015). As a form of "liberation technology", as Diamond (2010) notes, social media and other ICT applications enable "citizens to report news, expose wrong-doing, express opinions, mobilize protest, monitor elections, scrutinize government, deepen participation, and expand the horizons of freedom" (p. 70). While over-enthusiastic and technologically-deterministic notions of social media 'revolutions' have increasingly been criticised (Christensen, 2011; Morozov, 2011), many observers maintain that digital platforms have been "effective catalysts" (Khamis and Vaughn, 2011, p. 1) for change and amplifiers of social movement activism. They have lowered transaction costs for protest

movements, minimised necessary resources, enabled the creation of forums for free speech and for shared social and political criticism, and generated a social space for developing critical discourses where an open public sphere did not exist (Haunss, 2015).

Beyond the instrumental uses of social media for protest and activism, these observations point to the broader democratic and participatory potential of digital platforms which have been used for debate and creative peer production, and which have been key components of participatory cultures (Benkler, 2006; Jenkins, 2008). Innovations of digital culture, such as remixes and mash-ups, have broadened the creative engagement with people's cultural environment and have enhanced interactive potentials (Lessig, 2008). Further, the instances of activist and dissident uses of social media demonstrate significant overlaps and historical connections with other forms of social movement media (Downing, 2011), alternative media (Atton, 2001), community media (Rennie, 2006) and the broader range of 'our media' (Kidd et al., 2009). On a variety of platforms - from print to radio, and from the Internet to cassette tapes - these media have served as channels for dissident information and critical social debate. However, and in contrast to many of the more recent social networking platforms, these media practices have typically been self-organised and self-managed by civil society groups.

Social media services like Facebook and Google, on the other hand, are corporate platforms that operate under a commercial logic. As Leistert and Rohle (2011) note, their users are customers, not citizens. Social media are driven by necessary commercial considerations and the imperative of marketization, which means that user expectations for freedom of expression and privacy are only accepted as long as they concur with the commercial goals. Social media merge aspects of a public and private sphere (Papacharissi, 2010) as they allow people to engage in public and often democratic ways, but they do so through the means of a private media

environment. Similar to “the replacement of the downtown city centre by the shopping mall” (Andrejevic, 2012, p. 82), the privatised infrastructure of commercial social media offers a confined and controlled space for semi-public interactions, under the conditions of a commercial logic. Their architecture, policies and user terms must appeal to a broader public and may therefore enable activist uses (Youmans and York, 2012). However, centred around “a complex and dynamic set of highly opaque tools for selling advertisements, commodities and data” (Leistert, 2015, p. 35-36), their rationale contradicts the goals of many progressive social movements.

With a business model of collecting and analysing user data, social media are a “data mine” (Andrejevic, 2012, p. 71) that is at the heart of current surveillance trends, as highlighted by the Snowden leaks (Lyon, 2014). Social media platforms track detailed information about their users as well as their friends and acquaintances (Trottier and Lyon, 2012). The provision of a semi-public sphere of democratic communicative interactions and activist mobilisations aligns with this strategy as long as it offers the company increased access to user data and improves insights into the preferences, networks and activities of people. Accordingly, Facebook requires the use of ‘real names’ rather than pseudonyms and experiments with automatic facial recognition, which has led to significant problems for activists and their safety (Youmans and York, 2012). In contrast, activist-run non-profit platforms such as Indymedia have refused to store and monitor user data and thereby seek to protect the anonymity of their contributors.
The political economy of social media is marked by the dominant role of a small set of companies (Fuchs, 2014; Patelis, 2013) which often cultivate close and friendly interactions with the state (Assange, 2014), leading to cooperative and mutually supportive relations between the power centres of both Internet business and governance.

State Interventions: Social Media as an Object of Policing

The first area of concern for online dissent that I will address here are state interventions into both online content and Internet architecture. From a social movement perspective this is a classic source of constraints, whereas from an Internet perspective this may be less obvious. After all, many of the key components of the Internet were created "without a great deal of governmental or other oversight" (Cerf, 2004, p. 14) and focused on the end-to-end principle to empower the edges of the network, i.e. the user, rather than central nodes. "Governments of the Industrial World, leave us alone!", John Perry Barlow famously proclaimed in his Declaration of the Independence of Cyberspace: "You have no sovereignty where we gather" (Barlow, 1996). Cyberspace challenged the law's traditional reliance on territorial borders and thus questioned government's ability to control citizens' behaviour (Johnson and Post, 1996).

However, gradually such borders have been drawn around the previously borderless forms of cyberspace (Goldsmith and Wu, 2006). The 'Great Firewall of China' has demonstrated that control over major backbones and access points can allow governments to erect a virtual fence around a state territory and restrict access to both services and information from outside that territory (Deibert et al., 2008; Villeneuve, 2006). The Egyptian government, at the height of the Arab Spring uprising in January 2011, proved that Internet access in a country can be reduced or even shut down during protest situations, and other governments have applied this new capability with increasing frequency and flexibility (Webster, 2011). Inside a country's borders, filtering and blocking certain content has become common practice across the globe (Open Net Initiative, 2012). Information that transcends moral, religious or political limits set by governments has been blocked, most prominently in the Middle East and Asia, but increasingly

also in Western countries. For example, the system of 'Parental Control Filters' in the UK mandates Internet service providers to block a range of different content types deemed inappropriate for minors. Once censorship tools are in place, as Deibert (2009, p. 327) notes, "the temptation for authorities to employ them (..) for a wide range of ulterior purposes may be large." In countries as diverse as Thailand and Germany, the blocking of child pornography quickly led to demands for the filtering of a broader range of content deemed illegitimate (Hintz and Milan, 2011).

Social media services have been subject to wholesale blocking in countries such as China, Iran, Pakistan, Thailand and Turkey, and similar blocks have been discussed by Western governments (Deibert et al., 2008; Howard et al., 2011). While threats to national security and the preservation of cultural or religious morals serve typical rationales given for such action, many blocks have occurred as a direct reaction to protests, uprisings, and criticism of governments. They have thus served to protect political authority and mitigate dissidence. In many cases, "the targets (victims) are active domestic civic society movements" (Howard et al., 2011, p. 220).

While infrastructure-based restrictions to content and services directly affect the use of social media, defamation law and rules against incitement establish further constraints that are less immediate but may have serious consequences for the individual and may lead to a chilling effect on free expression. Prosecutions against bloggers and social media users for comments posted online have risen sharply - in Britain alone, at least 6,000 people a year were investigated between 2012 and 2015, in some cases leading to severe sentences (Bloodworth, 2015). These investigations concern a variety of offensive comments and hate speech, but definitions of what is deemed offensive depend on socio-political contexts. Criticism on social media of Western

military interventions in the Middle East, for example, has been interpreted as ‘promotion of terrorism’ and carried heavy sentences (Greenwald, 2015). Social media commentators on the London riots in August 2011 have been sentenced for incitement of violence (Guardian, 2011).

In many parts of the world, the users and producers of social media content have faced physical violence. Several dozen citizen journalists are reported killed every year, and in a number of countries they are tortured, ‘disappeared’, beaten or assaulted as a result of their online activity (Article 19, 2013). Even where their safety is not under threat, they often suffer from a precarious legal situation and do not enjoy the privileges of traditional journalists, such as protection against libel charges and the right to protect a source and collect certain types of information (Salter, 2009). Outside the realm of commercial services, activists who provide communications infrastructure for social movements have been subject to repression and the confiscation of equipment (Hintz and Milan, 2011). For example, servers used by the Indymedia network were seized by authorities in 2004 (following investigations by the FBI) and in 2005 by British police because of alleged incitement to criminal damage (Salter, 2009).

Social Media Censorship

Direct intervention by state authorities is increasingly complemented by the application of pressure on social media companies to police themselves. For example, Robert Hannigan, Director of the British Government Communications Headquarters (GCHQ), has called social media networks “terrorists’ command and control networks of choice” and singled out Internet companies for failing to address the misuse of their platforms by criminals and terrorists (Hannigan, 2014). Prime Minister David Cameron added that he would “step up pressure on web companies such as Facebook and Twitter to do more to co-operate with the intelligence

agencies" as they have a "social responsibility" to support governmental goals such as the fight against terrorism (Guardian, 2015a).

While such pressure may coerce social media platforms into stricter self-regulation, content interventions by Internet companies are not a new phenomenon and complement the regulations and requirements that stem from public policy. Terms of service constitute an additional regulatory framework that may go beyond the legality of content and often remains sufficiently vague so as to include any number of political or economic concerns. For example, rules to prevent 'indecency' caused Facebook to censor pictures of breastfeeding mothers, as well as cartoons depicting naked people, such as a naked Adam and Eve in the garden of Eden (Norton, 2014). Apple deleted an app from its app store that marked US drone strikes on a geographic map. The app was not illegal but certainly politically sensitive (Bonnington and Ackerman, 2012). Activists and political dissidents have experienced increasingly restrictive content policies as Facebook, for example, has discontinued activist pages in the run-up to protest events. Despite the platform's reputation for supporting protests and uprisings in the Middle East and elsewhere, it has taken down pages dedicated to anti-capitalist and anti-racist causes "as part of a growing effort by Facebook to crack down on the presence of political groups on its network" (Dencik, 2014). Activists may also be affected by increasing demands on social media to take down graphic content of violence against people, as documenting and circulating evidence of state violence has been both a key focus of citizen journalism and an important means for social movements to recruit new members to undertake collective action (Youmans and York, 2012).

Interventions, according to rules laid out in terms of service, take place alongside ongoing processes of the algorithmic sorting of content. Most social media companies are

adapting content feeds automatically according to their users' preferences and are therefore manipulating what users see in their news feeds. Facebook has actively experimented with affecting user behaviour regarding a core feature of the democratic system - voting. By providing selective information about voting behaviour by a user's friends, it has created statistically significant changes in voting patterns (Sifry, 2014). Changes to Google's ranking of search results can have similar effects as the relevant algorithm has profound implications for the visibility of online information. Incorporating the 'truthfulness' of an article in the search ranking, as was discussed in early 2015, may mean that mainstream narratives and official reports are highlighted whereas activist and dissident information which typically questions established 'truths' are moved down to the less visible search results (Watson, 2015). While these practices may not qualify as censorship by Internet companies, they have considerable impact on the availability of activist and political information on the web.

At the intersection between external interventions into, and internal interventions by, Internet companies, measures to report problematic content are sometimes used strategically to stifle dissent. For example, the Facebook Report Abuse button which allows users to flag content that is deemed inappropriate has been applied to report alleged 'abuse' by critical online publications, journalists, and activist Facebook groups whose accounts were taken down by Facebook as a consequence (Brandom, 2014).

If terms of service and interactions with both the state and other users can lead to content restrictions, so can interactions with other companies. The context of intellectual property violations shows how Internet companies have been the recipient and executor of take-down requests, as well as participating in the development of non-state rules and practices. Youtube, for example, responds to the uploading of potentially copyrighted materials to its platform on the

basis of agreements with copyright holders. Rather than waiting for a court order, its ContentID system detects copyrighted material and acts upon it in the way required by the respective agreement, which may mean to take it down or to monetize it. This form of content restriction does not focus on dissident and activist content. However the struggle over intellectual property has been a prominent theme of digital rights activism. In what has been termed the 'second enclosure' (Boyle, 2003), informational and immaterial goods have been commodified and transformed into markets, leading to "the making of knowledge and information into property" (May, 2009, p. 364). As control over ideas and knowledge has become a key economic resource and source of power, it affects the content available on social media and the very use of these platforms.

As we have seen, social media and other Internet companies have a gatekeeping function that may lead to restrictions on dissident or otherwise controversial content. As the services of commercial platforms extend beyond the sharing of information, apps and cultural goods to the provision of server space, domain registration and funding, these restrictions may affect the broader infrastructure of online communication. In December 2010, companies such as Amazon, Apple and Paypal demonstrated their gatekeeping role when they closed services they had previously provided for WikiLeaks, depriving this platform of its domain name and other public access points, and of access to necessary funds in the middle of a major release (the Cablegate leaks). This 'denial of service' (Benkler, 2011) demonstrated the significant power of so-called 'cloud' services in allowing and disallowing access to information and in controlling the gates that enable Internet users to participate in increasingly cloud-based communication exchanges. Further, these actions highlighted the vulnerability of commercial Internet services to political

interventions, as they coincided with pressure from members of the US political elite, both inside and outside government (Benkler, 2011).

Surveillance and the Social Media 'Data Mine'

The intersections between public and commercial interventions into online dissent are particularly prominent in the area of Internet surveillance. As electronic communication has vastly increased the capabilities of governments and corporate actors to monitor citizens' interactions, exchanges, locations and movements, targeted forms of surveillance have increasingly been replaced by the continuous collection and processing of information on wide areas of social life (Braman, 2006). In contemporary 'surveillance societies', "all manner of everyday activities are recorded, checked, traced and monitored" (Lyon, 2007). This has been demonstrated impressively by through revelations by whistleblower Edward Snowden about mass surveillance by security agencies such as the NSA and the GCHQ. Programmes such as Prism, Tempora, Muscular, Edgehill, Bullrun and Quantumtheory have provided evidence of mass surveillance of our social media uses; interception and monitoring of most online and phone communication; state-sponsored hacking into telecommunications services; the sabotage of security tools; and the compromising of Internet infrastructure (Guardian, 2015b).

The 'big data' generated through social media platforms is at the heart of current surveillance trends, as highlighted by the Snowden leaks (Lyon, 2014). As the business model of these companies is based on data collection, processing and monetization, it valorises surveillance (Cohen, 2008). The "data mine" (Andrejevic, 2012, p. 71) of social media allows for the detailed monitoring and analysis of Internet users, including their locations, activities, preferences, friends and networks, and political orientations. Applications (such as widgets and share buttons) that are included on an increasing number of websites allow the tracing of users

across the web, both by social media companies and their commercial partners. As social media render human connections measurable, information about people is not just inferred from their own activities and preferences but also from those of their friends and acquaintances (Trottier and Lyon, 2012). Unsurprisingly, Google, Facebook and others have been both at the centre of surveillance programmes such as Prism and in the spotlight of debate since the start of the revelations. Even before Snowden, Google documented in its Transparency Reports how governments use social media to collect information about its users. Google has received requests for the data of over 100 different users each day, in the US alone (Google Transparency Report, 2014). The contemporary surveillance assemblage (Haggerty and Ericson, 2000) thus consists of complex interactions between state and corporate actors.

Social media-based intelligence gathering (or SOCMINT) has become an important part of police investigations, including those that address activism and protest. Social media feeds are searched for keywords and particular 'threat words', and are analysed to identify both 'organisers' and 'influencers', i.e., those who spread information on protest and dissent across social media (Dencik et al., 2015). Even though SOCMINT is typically combined with pre-existing human intelligence and its analysis requires human intervention and discretion, its automated procedures and the core role of algorithms relate to growing concerns about algorithmic decision-making (e.g, Kitchin, 2014). It demonstrates how social media have become important tools for categorising people along social, economic and political lines, and how the marketing and advertising-oriented analysis of social media platforms is complemented by law enforcement investigations that inform predictive policing, for example of protests. The algorithms and analytical tools used for both purposes - marketing and police intelligence - are often the same (Dencik et al., 2015).

The consequences of social media surveillance have been felt, particularly, in the aftermath of 'social media revolutions' in the Middle East and elsewhere, where the use of platforms such as Facebook, Twitter and Youtube served as a means for the state to identify protesters and often put both their activities and their health and lives at risk. As Hofheinz (2011) notes about the 'Green Revolution' in Iran in 2009, "while people in New York cafés were forwarding tweets that gave them the thrilled feeling of partaking in a revolution, Iranian conservatives tightened their grip on power using YouTube videos and other Internet evidence to identify and arrest opposition activists" (p. 1420). In Iran, Tunisia, Syria and elsewhere, authorities have used social media to scrape user data and infect the computers of opposition supporters with spying software (Villeneuve, 2012). The Syrian government, at the beginning of the uprising in Syria, chose to unblock Facebook, Blogspot, and YouTube, which had been blocked since 2007, in order to increase surveillance (Youmans and York, 2012). Protesters in some places have quit social media, following arrests based on social media surveillance (Treré, 2015). Such experiences have raised questions about the 'sousveillance' (Mann et al., 2003) role of social media in counter-acting state and corporate 'surveillance'. Moreover, they highlight the 'chilling effect' of surveillance on free speech which undermines critical debate and dissident voices. Reports by the United Nations Special Rapporteur on Freedom of Expression and Opinion have consistently highlighted the fact that the right to privacy is an essential requirement for the realization of the right to freedom of expression (UN General Assembly, 2013).

Shifts in the Governance of Dissent and Free Expression

The ways in which social media serve as both objects and agents in the restriction of information and communication point us to transformations in the location of information control

and the governance of communication. They allow us to observe a shift in policymaking and regulation towards a larger role for private intermediaries.

As we can see, social media are sites through which the state enforces regulations, but they also formulate and enforce their own rules for acceptable user behaviour. In the area of content control, they have created platform-specific policies for accepting and rejecting content, which emerge from their commercial goals and are subject, to varying degrees, to influence by both user communities and the state. They have thus become a "social media police force" (Dencik, 2014) and act as "proxy censors" (Kreimer, 2006, p. 13) that are bound by their own commercial logics and political leanings, rather than civil rights and the rule of law. The context of communication on social media, and particularly the expression of dissent, is thus marked by a "transition from rights to express opinions to the necessity to fit within an often changing and intransparent regime of codes of conduct, terms of services and ownership" (Leistert, 2015, p. 36). Leistert has described this as a transformation from legality to benevolence (p. 36.).

The theme of surveillance highlights how the business practices of social media lead to increased user monitoring for both commercial and state goals. Both the Snowden leaks and corporate transparency reports have demonstrated the extent to which private intermediaries, and social media in particular, are now at the centre of state efforts to monitor citizens and Internet user behaviour. While some of the programmes revealed by Snowden (such as 'Muscular') have been used to intercept data traffic between the servers of social media companies without the latter's knowledge, the more prominent programmes (such as 'Prism' and 'Tempora') have relied on the knowledge and cooperation of Internet companies and telecommunications providers. Some post-Snowden policy changes, such as the USA Freedom Act, have further outsourced the collection and storage of data to social media companies, telecommunications

services and ISPs, and have thereby expanded the intersections and necessary interactions between Internet companies and state agencies. As data collection, mining and analysis plays an increasing role in contemporary forms of government (Leistert, 2015), social media delivers important functions.

The struggle around intellectual property violations offers particularly useful insights into the outsourcing of policy as it focuses largely on interactions between private companies. Youtube's ContentID system, as we saw above, acts upon copyrighted material as a result of agreements with copyright holders, rather than in reaction to court orders. Similarly, intellectual property owners or their representatives, such as the Recording Industry Association of America (RIAA), request ISPs or content providers to take down particular content. Such private sector-based processes have led to requests to remove, on average, 20-25 million URLs from Google searches each month, by summer 2014 (Google Transparency Report, 2014). So-called 'Graduated Response' policies to deter copyright infringement have increasingly included business agreements that place both the definition of, and the punishment for, copyright violations in the hands of content owners and ISPs. For example, the US Copyright Alert System has copyright holders identify shared copyrighted material and ISPs exert punishment by issuing a warning to the customer or, as a last resort, by cancelling their Internet connection altogether (Flaim, 2012). According to Mueller (2010), "the regulatory trend that constantly emerges from the [intellectual property] tension is a shift of the responsibility for monitoring and policing Internet conduct onto strategically positioned private sector intermediaries" (p. 149). By "delegating responsibility to the private sector", the state enlists businesses and other non-state actors in implementing communications policy and, furthermore, transfers quasi-policy functions (p. 149).

This privatisation of content regulation takes place in the context of broader trends in communications policy. Both the spaces and actors of policy-making have expanded over the past decades beyond the classic focus on national law and regulation. Developments taking place at other levels than the national, and both normative and material influences by a variety of non-state actors, have increasingly transformed traditional regulatory procedures. National policy has thus "become embedded within more expansive sets of interregional relations and networks of power" (Held and McGrew, 2003, p. 3), and policy authority is now located at "different and sometimes overlapping levels – from the local to the supra-national and global" (Raboy and Padovani, 2010, p. 16). Policy fora such as the World Summit on the Information Society (WSIS) and the Internet Governance Forum (IGF) have experimented with new forms of multi-stakeholder processes that include civil society and the business sector (Hintz, 2009). The main Internet governance institution, the Internet Corporation for Assigned Names and Numbers (ICANN), has relegated governments to an advisory function. Thus the vertical, centralized and state-based modes of traditional regulation have been complemented by collaborative horizontal arrangements, leading to "a complex ecology of interdependent structures" with "a vast array of formal and informal mechanisms working across a multiplicity of sites" (Raboy, 2002, p. 6-7).

Non-state actors - including both civil society networks and companies such as commercial social media - have engaged with this complex environment on a variety of levels. To start with, they have staged normative interventions into policy debate by setting agendas, exerting public pressure, lobbying and public campaigns, and by lending or withdrawing legitimacy to policy goals, decisions and processes (Keck and Sikkink, 1998). Google has invested over $13 million in lobbying activities in 2015 (Open Secrets, 2015). Further, Internet companies have changed the communications environment by developing new technologies and

platforms, and with them new standards, protocols and practices that have become de-facto cornerstones of communication technology. As technical standards and protocols typically allow some actions and disallow others, and enable some uses and restrict others, their development constitutes a latent and invisible form of policymaking (e.g., Braman, 2006; DeNardis, 2009; Lessig, 1999). The content standards that social media set through their terms of service and rule-making constitute a further set of standards that interacts with public policy and international norms and competes with these classic rules.

Like contemporary global governance, the privatised policy of social media companies connects the national with the regional and the global level. Companies are subject to domestic state policies and interact with the state through lobbying and various forms of collaboration (as described above). They have to comply with the laws and policies of other states and regions (such as the European Union) and they interact with global policy fora. Yet their services, and thus their specific technological and content standards as well as their data collection practices extend, potentially, to a global reach of users across states and regions.

Finally, the privatisation of communication policy in the form of an increased role for commercial intermediaries points to the broader trend of neoliberal restructuring, in which political authority and decision-making power are taken out of the public realm and transferred to private environments, often underpinned by commercial and market logics (Crouch, 2004).

Openings and Resistance

If social media platforms increasingly self-regulate content and user behaviour, in accordance with their commercial logics and profit goals, this changes the avenues of protest and resistance. While it becomes more difficult to appeal to public policy and human rights, campaigns against social media platforms have caused Internet companies to change their terms

of service and content policies. For example, the #FBrape campaign in 2013 led Facebook to moderate posts more rigidly that depict violence against women, as well as other 'cruel and insensitive' content. Crucially, the campaign had persuaded 15 brands to pull their advertising from the social network. Twitter followed soon by establishing anti-harassment tools and simplifying reporting processes for abusive tweets (Moyer, 2015).

Responses by digital rights activists and concerned customers to the Snowden revelations, similarly, have led Internet companies to improve user privacy and establish encrypted data transfers. US-based companies, in particular, have had to address customer concerns regarding data security in the context of NSA spying. Not least, this has created divisions between Internet companies and the state and has thus shaken up their previously cosy relations (Wizner, 2015). Projects such as 'Ranking Digital Rights' (https://rankingdigitalrights.org/) have advanced the focus on corporate policies by creating an 'Accountability Index' based on the policies and commitments of Internet and telecommunications companies regarding user privacy and freedom of expression.

Consumer action has thus made use of promising openings. However its limits have lied in its ad-hoc nature and its acceptance of the key role of corporate policy, which have left the broader issues and implications of privatised policy unaddressed. The response by social media companies to campaigns such as #FBrape may be particularly forthcoming if the solutions to the problem align with the companies' commercial self-interest. In this case, Facebook used the campaign to establish and justify its real-name policy which, as we have seen, has been damaging for many activists and alternative cultures.

Prefigurative action has taken one step further as a strategy of communications activism to address grievances. It shares with the kinds of consumer action mentioned above an approach

that does not focus on addressing established political venues, but implies a more fundamental transformation of both the development of, and the decision-making over, communications infrastructure. Prefigurative action in response to issues such as Internet censorship and surveillance include the development of technological alternatives that bypass regulatory obstacles, and reinforce autonomous and civil society-based media infrastructure. Rather than agitating for policy change, many Internet activists see their task as the creation of "self-managed infrastructures that work regardless of 'their' regulation, laws or any other form of governance" (Indymedia activist, in Hintz and Milan, 2009, p. 31). Their strategies focus on prefigurative action, rather than attempts to influence policy processes they regard as dominated by existing powers, and even extend their interventions to 'policy hacking' initiatives to develop new model laws and regulatory frameworks (Hintz, forthcoming; Hintz and Milan, 2013). In their efforts, they thus mirror privatised forms of policy authority and implementation as they trust in their own ability to develop solutions to perceived problems, rather than in the abilities of public institutions.

Conclusion

Social media and other digital platforms have provided an important means of activist and dissident communication, but they are also key sites where the tension between free communication and the emerging reality of restriction and censorship is played out. As the deterritorialised spheres of the Internet have partly been re-territorialised by states, practices of filtering and blocking content are expanding, illegalities of content are defined, and digital surveillance has become pervasive. Social media companies and other commercial intermediaries are subjected to these trends as they are enlisted by the state to police the net, and as they are required by governments to monitor their users and store data exchanges. Yet they

also play an active role in developing and enforcing new rules for allowing as well as restricting information; they define and punish objectionable user behaviour; and they provide and withdraw, accordingly, vital spaces and resources for communication. Further, they are placed at the centre of contemporary 'surveillance societies' as their business rationale requires the capturing, analysis and monetization of data and the commodification of users. For activists and providers of dissident information, the incorporation of social media into restrictive state policies and intelligence gathering routines, as well as the practices of intermediaries to set content standards and monitor user behaviour, provide a serious challenge and a significant shift as platforms used for protest and public debate are transformed into controlled spaces. What was regarded as 'liberation technology' is progressively enclosed.

The increasing role of private intermediaries in formulating, implementing and enforcing regulatory mechanisms demonstrates, as I have argued, a shift in the governance of speech. This shift is marked by the outsourcing of public policy to private actors and thus the privatisation of some policy areas. It includes both the establishment of competing policies, for example on content regulation, and collaborations between the state and private sectors, for example on surveillance. For activism and dissent, the relative weakening of state-based control of information has created openings. However the commercial logic of social media platforms and their close interactions with, and use by, state agencies has established new challenges.

References

Allan, S. (2013). *Citizen Witnessing: Revisioning Journalism in Times of Crisis.* Cambridge: Polity.

Andrejevic, M. (2012). Exploitation in the Data Mine. In: C. Fuchs, K. Boersma, A. Albrechtslund, and M. Sandoval (Eds.), *Internet and Surveillance: The Challenges of Web 2.0 and Social Media* (pp. 71-88). Abingdon: Routledge.

Article 19 (2013). *The Right to Blog, Policy Brief*. London: Article 19.

Assange, J. (2014). *When Google Met WikiLeaks*. OR Books.

Atton, C. (2001). *Alternative Media.* London: Sage.

Barlow, J. P. (1996). A declaration of the independence of cyberspace. Retrieved from http://homes.eff.org/~barlow/Declaration-Final.html

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

Benkler, Y. (2011). A Free Irresponsible Press: WikiLeaks and the Battle over the Soul of the Networked Fourth Estate. Retrieved from: http://www.benkler.org/Benkler_Wikileaks_current.pdf

Bloodworth, J. (2015, January 1). Katie Hopkins' views are now considered matters for law enforcement, and it is utterly terrifying. *Independent*. Retrieved from: http://www.independent.co.uk/voices/comment/katie-hopkins-views-are-now-considered-matters-for-law-enforcement-and-it-is-utterly-terrifying-9953339.html

Bonnington, C., and Ackerman, S. (2012, August 30). Apple Rejects App that Tracks U.S. Drone Strikes. *Wired*. Retrieved from: http://www.wired.com/2012/08/drone-app/

Boyle, J. (2003). The second enclosure movement and the construction of the public domain. *Law and Contemporary Problems,* 66 (1-2), 33-74.

Braman, S. (2006). *Change of State: Information, Policy, and Power.* Cambridge: MIT Press.

Brandom, R. (2014, September 2). Facebook's Report Abuse button has become a tool of global oppression. *The Verge*. Retrieved from: http://www.theverge.com/2014/9/2/6083647/facebook-s-report-abuse-button-has-become-a-tool-of-global-oppression

Cerf, V. G. (2004). First, do no harm. In D. MacLean (Ed.), *Internet Governance: A Grand Collaboration* (pp. 13-15). New York: United Nations ICT Task Force.

Christensen, C. (2011). Twitter Revolutions? Addressing Social Media and Dissent. *The Communication Review,* 14 (3), 155-157.

Cohen, N. (2008). The valorization of surveillance: Towards a political economy of Facebook. *Democratic Communiqué,* 22 (1), 5-22.

Crouch, C. (2004). *Post-Democracy.* Cambridge: Polity.

Deibert, R. (2009). The geopolitics of internet control: censorship, sovereignty, and cyberspace. In A. Chadwick and P. Howard (Eds.), *The Routledge Handbook of Internet Politics* (pp. 323-336). London: Routledge.

Deibert, R. J., Palfrey, J. G., Rohozinski, R., and Zittrain, J. (2008). *Access Denied: The Practice and Policy of Global Internet Filtering.* Cambridge: MIT Press.

DeNardis, L. (2009). *Protocol Politics: The Globalization of Internet Governance.* Cambridge: MIT Press.

Dencik, L. (2014, January 13). Why Facebook Censorship Matters. *JOMEC Blog.* Retrieved from: http://www.jomec.co.uk/blog/why-facebook-censorship-matters/

Dencik, L., and Leistert, O. (2015). Introduction. In L. Dencik and O. Leistert (Eds.), *Critical Perspectives on Social Media and Protest: Between Control and Emancipation* (pp. 1-12). Lanham: Rowman and Littlefield.

Dencik, L., Hintz, A., Carey, Z., and Pandya, H. (2015). Managing 'Threats': Uses of Social Media for Policing Domestic Extremism and Disorder in the UK. Project report. Cardiff University. Retrieved from: http://www.dcssproject.net/files/2015/12/Managing-Threats-Project-Report.pdf

Diamond, L. (2010). Liberation Technology. *Journal of Democracy*, 21 (3), 69-83.

Downing, J. D. H. (Ed.) (2011). *Encyclopedia of Social Movement Media.* London: Sage.

Flaim, S. M. (2012, April). Op-ed: Imminent 'six strikes' Copyright Alert System needs antitrust scrutiny. *Ars technica*. Retrieved from: http://arstechnica.com/tech-policy/news/2012/03/op-ed-imminent-six-strikes-copyright-alert-system-needs-antitrust-scrutiny.ars

Fuchs, C. (2014). *Social Media: A Critical Introduction.* London: Sage.

Goldsmith, J., and Wu, T. (2006). *Who Controls the Internet? Illusions of a Borderless World.* Oxford: Oxford University Press.

Google Transparency Report (2014). http://www.google.co.uk/transparencyreport/

Greenwald, G. (2015, January 2006). With Power of Social Media Growing, Police Now Monitoring and Criminalizing Online Speech. *The Intercept*. Retrieved from: https://firstlook.org/theintercept/2015/01/06/police-increasingly-monitoring-criminalizing-online-speech/

Guardian (2011, August 16). Facebook riot calls earn men four-year jail terms amid sentencing outcry. *Guardian*. Retrieved from: http://www.guardian.co.uk/uk/2011/aug/16/facebook-riot-calls-men-jailed

Guardian (2015a, January 16). Facebook and Twitter have social responsibility to help fight terrorism, says Cameron. *Guardian*. Retrieved from:

http://www.theguardian.com/world/2015/jan/16/cameron-interrupt-terrorists-cybersecurity-cyberattack-threat

Guardian (2015b). The NSA Files. *Guardian*. Retrieved from: http://www.theguardian.com/us-news/the-nsa-files

Haggerty, K. D., and Ericson, R. V. (2000). The surveillant assemblage. *British Journal of Sociology*, 51 (4), 605-622.

Hannigan, R. (2014, November 3). The Web is a terrorist's command-and-control network of choice. *Financial Times*. Retrieved from: http://www.ft.com/cms/s/2/c89b6c58-6342-11e4-8a63-00144feabdc0.html#axzz3TywRsOQ2

Haunss, S. (2015). Promise and Practice in the Study of Social Media and Movements. In L. Dencik and O. Leistert (Eds.), *Critical Perspectives on Social Media and Protest: Between Control and Emancipation* (pp. 13-34). Lanham: Rowman and Littlefield.

Held, D., and McGrew, A. C. (2003). The Great Globalization Debate. In D. Held and A. G. McGrew (Eds.), *The Global Transformations Reader* (pp. 1-50). Cambridge: Polity Press.

Hintz, A. (2009). *Civil Society Media and Global Governance: Intervening into the World Summit on the Information Society*. Münster: LIT.

Hintz, A. (2014). Independent Media Center. In: K. Harvey (Ed.), *Encyclopedia of Social Media and Politics* (pp. 653-654). London: SAGE.

Hintz, A. (forthcoming). Policy Hacking: Citizen-based Policymaking and Media Reform. In D. Freedman and R. McChesney (Eds.), *Strategies for Media Reform: International Perspectives.* New York: Fordham University Press.

Hintz, A., and Milan, S. (2009). At the Margins of Internet Governance: Grassroots Tech Groups and Communication Policy. *International Journal of Media & Cultural Politics*, 5 (1), 23-38.

Hintz, A., and Milan, S. (2011). User Rights for the Internet Age: Communications Policy According to Netizens. In R. Mansell and M. Raboy (Eds.), *The Handbook of Global Media and Communication Policy* (pp. 230-241). Oxford: Wiley-Blackwell.

Hintz, A., and Milan, S. (2013). Networked Collective Action and the Institutionalised Policy Debate: Bringing Cyberactivism to the Policy Arena? *Policy & Internet*, 5 (1), 7-26.

Hofheinz, A. (2011). Nextopia? Beyond Revolution 2.0. *International Journal of Communication*, 5. Retrieved from: http://ijoc.org/ojs/index.php/ijoc/article/view/1186

Howard, P. N., Agarwal, S. D., and Hussain, M. M. (2011). When Do States Disconnect Their Digital Networks? Regime Responses to the Political Use of Social Media. *The Communication Review*, 14 (3), 216-232.

Jenkins, H. (2008). *Convergence Culture: Where Old and New Media Collide*. New York: New York University Press.

Johnson, D. R., and Post, D. (1996). Law and borders: The rise of law in cyberspace. *Stanford Law Review*, 48 (5), 1367-1402.

Keck, M. E., and Sikkink, K. (1998). *Activists beyond Borders. Advocacy Networks in International Politics*. Ithaca: Cornell University Press.

Khamis, S., and Vaughn, K. (2011). Cyberactivism in the Egyptian Revolution: How Civic Engagement and Citizen Journalism Tilted the Balance. *Arab Media & Society*, 14.

Kidd, D., Rodriguez, C., and Stein, L. (Eds.). (2009). *Making Our Media: Global Initiatives Toward a Democratic Public Sphere*. Cresskill: Hampton Press.

Kitchin, R. (2014). Thinking critically about and researching algorithms. *The Programmable City*, Working Paper 5.

Kreimer, S. F. (2006). Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link. *University of Pennsylvania Law Review*, 155 (11).

Leistert, O., and Rohle, T. (2011). Identifizieren, Verbinden, Verkaufen. Einleitendes zur Maschine Facebook, ihren Konsequenzen und den Beiträgen in diesem Band. In O. Leistert and T. Rohle (Eds.), *Generation Facebook: Über das Leben im Social Net* (pp. 7-30). Bielefeld: Transcript.

Leistert, O. (2015). The Revolution Will Not Be Liked: On the Systematic Constraints of Corporate Social Media Platforms for Protest. In L. Dencik and O. Leistert (Eds.), *Critical Perspectives on Social Media and Protest: Between Control and Emancipation* (pp. 35-52). Lanham: Rowman and Littlefield.

Lessig, L. (1999). *Code and other Laws of Cyberspace.* New York: Basic Books.

Lessig, L. (2008). *Remix: Making Art and Commerce Thrive in the Hybrid Economy.* London: Bloomsbury.

Lyon, D. (2007). Surveillance, Power, and Everyday Life. In R. Mansell, C. Anthi Avgerou, D. Quah and R. Silverstone (Eds.), *The Oxford Handbook of Information and Communication Technologies* (pp. 449-472). Oxford: Oxford University Press.

Lyon, D. (2014). Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique. *Big Data & Society*, July-December, 1-13.

Mann, S., Nolan, J., and Wellman, B. (2003). Sousveillance: inventing and using wearable computing devices for data collection in surveillance environments. *Surveillance and Society*, 1 (3), 331-355.

May, C. (2009). Globalizing the logic of openness: open source software and the global governance of intellectual property. In A. Chadwick and P. Howard (Eds.), *The Routledge Handbook of Internet Politics* (pp. 364-375). London: Routledge.

Morozov, E. (2011). *The Net Delusion: The Dark Side of Internet Freedom*. New York: Public Affairs.

Moyer, E. (2015, November 8). Twitter teams with women's group on anti-harassment tool. *Cnet*. Retrieved from: http://www.cnet.com/news/twitter-teams-up-with-womens-group-on-anti-harassment-tool

Mueller, M. (2010). *Networks and States: The Global Politics of Internet Governance.* Cambridge: MIT Press.

Norton, B. (2014, January 10-12). Fascist Facebook? The Social Network Giant's Double Standards. *Counterpunch*. Retrieved from: http://www.counterpunch.org/2014/01/10/fascist-facebook/

Open Secrets (2015, October 23). Google Inc. Retrieved from: https://www.opensecrets.org/lobby/clientsum.php?id=D000022008

Open Net Initiative (2012, April 3). Global Internet Filtering in 2012 at a Glance. *Open Net*. http://opennet.net/blog/2012/04/global-internet-filtering-2012-glance

Papacharissi, Z. (2010). *A Private Sphere: Democracy in a Digital Age*. Cambridge: Polity.

Patelis, K. (2013). Political Economy and Monopoly Abstractions: What Social Media Demand. In G. Lovink and M. Rasch (Eds.) *Unlike Us Reader: Social Media Monopolies and their Alternatives* (pp. 117-126). Amsterdam: Institute of Network Cultures.

Raboy, M. (2002). *Global Media Policy in the New Millennium.* Luton: University of Luton Press.

Raboy, M., and Padovani, C. (2010). Mapping Global Media Policy: Concepts, Frameworks, Methods. Retrieved from: http://www.globalmediapolicy.net/sites/default/files/Raboy&Padovani%202010_long%20version_final.pdf

Rennie, E. (2006). *Community Media: A Global Introduction*. Lanham: Rowman & Littlefield.

Salter, L. (2009). Indymedia and the Law: Issues for Citizen Journalism. In S. Allan and E. Thorsen (Eds.), *Citizen Journalism: Global Perspectives* (pp. 175-186). New York: Peter Lang.

Sifry, M. (2014, October 31). Facebook wants you to vote on Tuesday. Here's how it messed with your feed in 2012. *Mother Jones*. Retrieved from: http://www.motherjones.com/politics/2014/10/can-voting-facebook-button-improve-voter-turnout

Trere, E. (2015). The Struggle Within: Discord, Conflict and Paranoia in Social Media Protest. In L. Dencik and O. Leistert (Eds.), *Critical Perspectives on Social Media and Protest: Between Control and Emancipation* (pp. 163-180). Lanham: Rowman and Littlefield.

Trottier, D. and Lyon, D. (2012). Key Features of Social Media Surveillance. In C. Fuchs, K. Boersma, A. Albrechtslund, and M. Sandoval (Eds.) *Internet and Surveillance: The Challenges of Web 2.0 and Social Media* (pp. 89-105). Abingdon: Routledge.

UN General Assembly (2013, April 17). Report of the Special Rapporteur on the promotion and protection of the right to freedom of expression. Frank La Rue. Retrieved from: http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

Villeneuve, N. (2006). The filtering matrix: Integrated mechanisms of information control and the demarcation of borders in cyberspace. *First Monday*, 11 (1-2). Retrieved from: http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1307/1227.

Villeneuve, N. (2012, April 20). Fake Skype Encryption Software Cloaks DarkComet Trojan. *Trend Micro Malware Blog*. Retrieved from: http://blog.trendmicro.com/fake-skype-encryption-software-cloaks-darkcomet-trojan/

Watson, S. (2015, March 2). Google Moving to Shut Down Alternative Media by Ranking Sites on 'Facts' Rather than Popularity. *Global Research*. Retrieved from: http://www.globalresearch.ca/google-moving-to-shut-down-alternative-media-by-ranking-sites-on-facts-rather-than-popularity/5434328

Webster, S. C. (2011, January 28). Vodaphone confirms role in Egypt's cellular, Internet blackout. *The Raw Story*. Retrieved from: http://www.rawstory.com/rs/2011/01/28/vodafone-confirms-role-egypts-cellular-internet-blackout/

Wizner, B. (2015). Keynote address to the conference 'Surveillance and Citizenship', Cardiff, 18 June.

Youmans, W. L., and J. C. York (2012). Social Media and the Activist Toolkit: User Agreements, Corporate Interests, and the Information Infrastructure of Modern Social Movements. *Journal of Communication*, 62, 315-329.