Outsourcing Surveillance—Privatising Policy: Communications Regulation by Commercial Intermediaries

ARNE HINTZ*

The Snowden revelations of mass online surveillance have provided unprecedented information on state-based surveillance mechanisms. However they have also directed our attention to the role of commercial actors and private intermediaries. Commercial social media platforms are engaged in large-scale data collection and have been at the core of several NSA/GCHQ programmes—sometimes unknowingly, sometimes reluctantly, sometimes willingly.

This article will discuss the role of private actors in surveillance strategies within the wider context of the privatisation of communication policy. It will demonstrate how intermediaries have not only been assigned a greater role in implementing laws and regulations, but have moved towards actively formulating and setting policy that deeply affects freedom of expression and data protection. I will discuss the implications for both legal and democratic processes, highlighting the problem of outsourcing control over key civic rights.

I will situate this emerging authority of commercial actors in broader trends of communication policy that include networked multi-stakeholder processes, standard-setting by technical developers, and civil society practices of developing model laws and regulatory proposals as a form of 'DIY policy-making'.

* Cardiff University (email: hintza@cardiff.ac.uk). This article is based on research which is being conducted as part of the ESRC-funded project 'Digital Citizenship and Surveillance Society: UK State-Media-Citizen Relations after the Snowden Leaks' <http://blogs.cardiff.ac.uk/dcssproject>.

Introduction

The revelations by whistleblower Edward Snowden of mass online surveillance have provided unprecedented information on state-based surveillance mechanisms. However, they have also directed our attention to broader trends in communications policy. At the core of several of the surveillance programmes by the NSA and GCHQ are commercial social media platforms that are engaged in large-scale data collection. Sometimes unknowingly, sometimes reluctantly, sometimes willingly, they have provided key infrastructure for monitoring and analysing citizens' communication activities.

Social media companies' involvement in surveillance practices demonstrates how private intermediaries are increasingly enlisted in regulatory mechanisms and in the policing of online communication. Social media companies have restricted content that is published on or distributed through their platforms; resource and infrastructure providers have excluded clients (such as activist and oppositional information providers) from their services; and new intellectual property protection mechanisms have transferred the authority to define, detect and punish alleged copyright infringements to private actors (such as copyright holders and internet service providers).

This article will discuss the role of private actors in surveillance and other current issues in digital communication, and thus explore the privatization of communications policy. It will trace how intermediaries have not only been assigned a greater role in implementing laws and regulations, but have moved towards actively formulating and setting policy. It will situate the emerging authority of these actors in the broader debate on freedom of expression on the internet and in current trends of policymaking, such as multi-stakeholder policy processes, policy advocacy by both civil society and the private sector, and standard-setting by technical developers and infrastructure providers.

I will first outline this context by pointing to different dimensions of networked governance. Then I will highlight key areas of the current debate around internet freedoms and restrictions, focusing on the three areas of surveillance, censorship and intellectual property. The third section will emphasize the role of commercial platforms and

private intermediaries in those areas, while the fourth section will trace and analyse resistance to and contestation of these trends. I will argue that the trend of outsourcing regulatory decisions and privatising policy has serious implications for freedom of expression and data protection, and that this trend is mirrored by contestations and resistance that take place, equally, in the arena of private, non-state media actors and infrastructures.

Communications Policy and Networked Governance

Classic national lawmaking increasingly intersects with developments taking place at other levels and is subject to both normative and material influences by a variety of non-state actors. It has 'become embedded within more expansive sets of interregional relations and networks of power',[1] and policy is now located at 'different and sometimes overlapping levels – from the local to the supra-national and global'.[2] Policy fora such as the World Summit on the Information Society (WSIS) and the Internet Governance Forum have experimented with new forms of multi-stakeholder processes that include civil society and the business sector. The vertical, centralized and state-based modes of traditional regulation have thus 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'.[3]

Despite a lack of actual authority to adopt laws and regulations, non-state actors have been able to use this complex environment for

[1] David Held and Anthony G McGrew, 'The Great Globalization Debate' in David Held and Anthony G McGrew (eds), *The Global Transformations Reader* (Polity Press 2003) 3.

[2] Marc Raboy and Claudia Padovani, 'Mapping Global Media Policy: Concepts, Frameworks, Methods' (*Global Media Policy*, June 2010) 16 <http://www.globalmediapolicy.net/sites/default/files/Raboy&Padovani%202010_long%20version_final.pdf> accessed 2 December 2014.

[3] Marc Raboy, *Global Media Policy in the New Millennium* (University of Luton Press 2002) 6-7.

interventions into the 'consensus mobilization'[4] dynamics of policy debate. They define problems, set agendas, exert public pressure, sometimes through lobbying and public campaigns, sometimes by participating in multi-stakeholder policy development, and they hold significant leverage by lending or withdrawing legitimacy to policy goals, decisions and processes.[5] During 'policy windows', i.e. favourable institutional, political and sometimes ideological settings, such as economic crises and political change, they can affect policy change significantly.[6]

In addition to normative interventions, civil society groups and the business sector have changed the communications environment by developing new technologies and platforms, and with them new standards, protocols and practices that became de facto cornerstones of communication technology. Technical communities have engaged in these forms of latent and invisible 'policy-making' during, for example, the development of the internet and its technical standards and protocols, from TCP/IP to http to jpeg. Each of these allows some actions and disallows others, enables some uses and restricts others, and therefore occupies quasi-policy functions (see, for example, Lessig,[7] Braman,[8] and DeNardis[9]). Media activists, equally, have focused on the creation of alternative infrastructure that bypasses regulatory obstacles instead of lobbying against those obstacles. Rather than campaigning for privacy rights and against online surveillance, many of them have developed communication platforms (e.g., specific email services, social media, etc.) that respect

[4] Sanjeev Khagram, James V Riker and Kathryn Sikkink, 'From Santiago to Seattle: Transnational Advocacy Groups Restructuring World Politics' in Sanjeev Khagram, James V Riker and Kathryn Sikkink (eds), *Restructuring World Politics: Transnational Social Movements, Networks, and Norms* (University of Minnesota Press 2002) 11.

[5] Margaret E Keck and Kathryn Sikkink, *Activists Beyond Borders: Advocacy Networks in International Politics* (Cornell University Press 1998).

[6] John W Kingdon, *Agendas, Alternatives, and Public Policy* (Little, Brown & Co 1984).

[7] Lawrence Lessig, *Code and Other Laws of Cyberspace* (Basic Books 1999).

[8] Sandra Braman, *Change of State: Information, Policy, and Power* (MIT Press 2006).

[9] Laura DeNardis, *Protocol Politics: The Globalization of Internet Governance* (MIT Press 2009).

user privacy, and, rather than advocating for broadcast licences, many of them broadcast their own unlicensed 'pirate' radio. Interactions with the policy environment, in this case take place neither through lobbying 'inside' nor protesting 'outside' institutional or governmental processes, but through prefigurative action that creates alternative infrastructure and by adopting a tactical repertoire of circumvention.[10]

Business actors have, for a long time, been engaged with these different forms of policy interventions. During the early development of international radio standards, for example, they drafted declarations that were later adopted by government representatives, and they shaped the radio as a unidirectional broadcast medium by pursuing certain avenues of technological development and neglecting others.[11] They are heavily engaged with contemporary internet debates, from promoting certain standards and platforms (e.g. operating systems) to involvement with public campaigns (e.g. on intellectual property protection) and to intense lobbying (e.g. on net neutrality).

Surveillance, Censorship, and Other Challenges to Digital Communication

'Governments of the Industrial World, leave us alone!', John Perry Barlow proclaimed in his Declaration of the Independence of Cyberspace: 'You have no sovereignty where we gather'. [12] Cyberspace challenged the law's traditional reliance on territorial borders and thus questioned governments' ability to control citizens'

[10] Arne Hintz and Stefania Milan, 'At the Margins of Internet Governance: Grassroots Tech Groups and Communication Policy' (2009) 5(1) *International Journal of Media & Cultural Politics* 23; Stephania Milan, *Social Movements and their Technologies: Wiring Social Change* (Palgrave MacMillan 2013).

[11] Cees J Hamelink, *The Politics of World Communication: A Human Rights Perspective* (Sage 1994).

[12] John Perry Barlow, 'A Declaration of the Independence of Cyberspace' (8 February 1996) <http://homes.eff.org/~barlow/Declaration-Final.html> accessed 2 December 2014.

behaviour.[13] Anonymity was a possibility, if not the standard, of online communication, and as a famous *New Yorker* cartoon from 1993 pointed out: 'On the Internet, nobody knows you're a dog.' The end-to-end principle of the internet gave maximum power and control to the edges of the network, i.e., to the user, rather than central nodes. The development of standards and protocols largely happened in a decentralized, informal and experimental fashion by technologists rather than governments and as 'bottom-up, grassroots processes',[14] 'without a great deal of governmental or other oversight'.[15]

However, states and larger business actors have gradually (re)gained influence over the new virtual landscapes, particularly since the turn of the millennium.[16] In few areas has this change been as stark as in the practice of surveillance. In contrast to earlier celebrations (or concerns, depending on the perspective) of anonymity, electronic communication has vastly increased the capabilities of governments and corporate actors to monitor citizens' interactions, exchanges, locations and movements. In contemporary 'surveillance societies', 'all manner of everyday activities are recorded, checked, traced and monitored'.[17] As Sandra Braman notes, the traditional notion of panopticon-style surveillance has been replaced with the 'panspectron', in which information is gathered about everything, all the time.[18]

The revelations by whistleblower Edward Snowden about mass surveillance by security agencies such as the NSA and the GCHQ

[13] David R Johnson and David G Post, 'Law and Borders: The Rise of Law in Cyberspace' (1996) 48(5) Stanford Law Review 1367.

[14] Robert E Kahn, 'Working Code and Rough Consensus: The Internet as Social Evolution' in Don MacLean (ed), *Internet Governance: A Grand Collaboration,* (United Nations ICT Task Force 2004) 18.

[15] Vinton G Cerf, 'First, Do No Harm' in Don MacLean (ed), *Internet Governance: A Grand Collaboration* (United Nations ICT Task Force 2004) 14.

[16] Jack Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (Oxford University Press 2006).

[17] David Lyon, 'Surveillance, Power, and Everyday Life' in Phillip Kalantzis-Cope and Karim Gherab-Martin (eds), *Emerging Digital Spaces in Contemporary Society. Properties of Technology* (Palgrave Macmillan 2011) 7.

[18] Sandra Braman (n 8) 315.

have demonstrated this impressively. Programmes such as Prism, Tempora, Muscular, Edgehill, Bullrun and Quantumtheory have provided evidence of mass surveillance of social media users; 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. They have included paying security software firms to weaken the security of their products, and infecting citizens' computers with malware to see their screen or use their webcam. The extent to which this has allowed states and corporate actors to collect, store and analyse data amounts to—in the words of Barlow—'monitoring the communication of the human race'.[19]

National and international law has expanded governments' ability to monitor citizens' communication. For example the European Union Data Retention Directive, which was adopted in 2006 and implemented by most European countries in 2009 (but revoked by the European Court of Human Rights in 2014), required telecommunications operators and internet service providers to store their customers' connection data and to make it available to the authorities upon request. This concerns detailed information on who communicates with whom, at what times, for how long, and at which physical location. According to civil rights lawyer T J McIntyre, the Directive resulted in the creation of 'a comprehensive digital dossier about every individual'.[20] In the wake of the Snowden revelations, states have replaced the Directive with national law and have expanded the legality of data collection further—for example, in the UK, through the controversial Data Retention and Investigatory Powers Act 2014.

Blanket surveillance and pervasive monitoring of people's movements, actions and communication undermine critical debate and dissident voices, and thus key features of a functioning democracy. Just a few days before the first Snowden leaks were

[19] Interview by Sky News with John Perry Barlow and Julian Assange (*Sky News*, 10 June 2013) <www.youtube.com/watch?v=_DO8mdrPYWw> accessed 3 December 2014.

[20] T J McIntyre, 'Data Retention in Ireland: Privacy, Policy and Proportionality' (2008) 24(4) Computer Law & Security Report 326, 327.

published in June 2013, the United Nations Special Rapporteur on Freedom of Expression and Opinion delivered a landmark report on state surveillance and freedom of expression in which he highlighted that the right to privacy is an essential requirement for the realization of the right to freedom of expression.[21] Critical and investigative reporting is particularly challenged by surveillance, as it requires confidential communication with sources and, occasionally, the anonymity of authors.[22]

A second area of significant change has been the drawing of territorial borders, and thus the (re)introduction of classic territorial law, in cyberspace. The 'Great Firewall of China' has demonstrated that control over major backbones and access points can allow governments to draw a virtual fence around a state territory and restrict access to both services and information from outside that territory.[23] 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.[24] Inside a country's borders, filtering and blocking certain content has become common practice across the globe.[25] Information that transcends moral, religious or political limits set by governments has been blocked, most

[21] UNGA, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Expression (Frank La Rue)' (17 April 2013) UN Doc A/HRC/23/40.

[22] Alan Rusbridger, 'David Miranda, Schedule 7, and the Danger that All Reporters Now Face' (*The Guardian*, 19 August 2013) <www.theguardian.com/commentisfree/2013/aug/19/david-miranda-schedule7-danger-reporters> accessed 3 December 2014.

[23] Ronald Deibert, John Palfrey, Rafal Rohozinski and Jonathan Zittrain (eds), *Access Denied: The Practice and Policy of Global Internet Filtering* (MIT Press 2008).

[24] Stephen C Webster, 'Vodafone Confirms Role in Egypt's Cellular, Internet Blackout' (*The Raw Story*, 28 January 2011) <www.rawstory.com/rs/2011/01/28/vodafone-confirms-role-egypts-cellular-internet-blackout/> accessed 3 December 2014.

[25] OpenNet Initiative, 'Global Internet Filtering in 2012 at a Glance' (*OpenNet Initiative*, 3 April 2012) <http://opennet.net/blog/2012/04/global-internet-filtering-2012-glance> accessed 3 December 2014.

prominently in the Middle East and Asia, but increasingly also in Western countries. The UK has occupied a questionable pioneer role as internet service providers, mandated by the government, have established 'Parental Control Filters' that censor a range of different content types deemed inappropriate for minors.

While child protection and the restriction of, for example, child pornography, may be admirable goals, the creation of an extensive censorship architecture for these purposes typically raises demands for wider content restrictions. As Ron Deibert notes, 'once the tools of censorship are in place, the temptation for authorities to employ them for a wide range of purposes are large'.[26] In Thailand, for example, the initial blocking of pornographic material was gradually extended to politically sensitive material. Some of the UK filters have included vague categories such as 'extremist related content' and 'esoteric material' which are open for wide interpretation. The adoption of a child pornography filtering law in Germany in 2009 was quickly followed by demands to extend the law to a broader range of content deemed illegitimate.[27] But filtering can also lead to unintended over-blocking because of the imperfections or technical configuration of the software. An attempt by an internet service provider in Canada, for example, to block one site caused more than 600 non–related websites to be blocked,[28] and the child protection filters in the UK have blocked access to, for example, sexual education websites, parental guidance sites, the support site childline.org.uk, and the website of the Electronic Frontier Foundation, an important digital rights advocacy organization co-founded by John Perry Barlow.[29]

---

[26] Ronald J Deibert, 'The Geopolitics of Internet Control: Censorship, Sovereignty, and Cyberspace' in Andrew Chadwick and Philip N Howard (eds), *The Routledge Handbook of Internet Politics* (Routledge 2009).

[27] Hintz and Milan, 'At the Margins of Internet Governance' (n 10).

[28] Nart Villeneuve, 'The Filtering Matrix: Integrated Mechanisms of Information Control and the Demarcation of Borders in Cyberspace' (2006) 11(1) First Monday <http://ojs-prod-lib.cc.uic.edu/ojs/index.php/fm/article/view/1307/1227> accessed 3 December 2014.

[29] Martin Robbins, 'Cameron's Internet Filter Goes Far Beyond Porn—And That Was Always the Plan' (*New Statesman*, 23 December 2013)

Content restrictions include the increasing criminalization of defamation online and tighter restrictions to speech that may include incitement. Many recent laws against the incitement to violence, crime and terrorism have been vague and open to subjective interpretations, which has led, for example in the UK, to a steep rise in prosecutions against bloggers and social media users for comments posted online. In some countries, special criminal sanctions have been introduced for online defamation.[30]

A more indirect form of content restrictions has emerged with the debate on net neutrality. As a network of cables and wireless connections that move data packages from A to B regardless of their content, the internet has largely been a neutral platform for information exchange, rather than a broadcaster that makes editorial decisions. As such, it has become an important public sphere and a crucial space for free expression and democratic participation.[31] However the increasing practise by ISPs and telecommunications services of blocking and/or throttling (i.e. slowing down) some content, and speeding up the delivery of other content and services, has substantially altered this space. This form of content discrimination through infrastructure control provides particular challenges for non-commercial content and small businesses that may not be able to pay the fee required to be on a 'fast lane', and for oppositional and dissident news sources whose exposure a network provider may want to limit.[32]

Finally, the increasingly rigid interpretation (and enforcement) of intellectual property has led to further restrictions. The free availability of protocols and standards has been essential for how we use the net today, and the hacker slogan 'information wants to be

<www.newstatesman.com/politics/2013/12/camerons-internet-filter-goes-far-beyond-porn-and-was-always-plan> accessed 3 December 2014.

[30] Article 19, 'The Right to Blog: Article 19 Policy Brief' (*Article 19*, 2013) <www.article19.org/data/files/medialibrary/3733/Right-to-Blog-EN-WEB.pdf> accessed 4 December 2014.

[31] Maria Loeblich and Francesca Musiani, 'Net Neutrality and Communication Research: The Implications of Internet Infrastructure for the Public Sphere' in Elisia L Cohen (ed), *Communication Yearbook 38* (Routledge 2014).

[32] Jack M Balkin, 'The Future of Free Expression in a Digital Age' (2009) 36(2) Pepperdine Law Review 427.

free' has been a cornerstone for infrastructure development, the emergence of free and open source software, and aspects of digital culture such as remixes and mash-ups.[33] The internet is a 'gigantic, globally distributed, always-on copying machine',[34] and a huge library that allows us to share files, share knowledge, and benefit from an abundance of ideas. However, control over these ideas and knowledge through the means of intellectual property has become a key economic resource and source of power and is therefore enforced fiercely. In what has been termed the 'second enclosure',[35] knowledge and information have been commodified and put under the control of the business sector. As scarcity—and thus a market—is created for informational and immaterial goods, we have witnessed 'the making of knowledge and information into property'.[36] The state has regulated and supported this process through the draconian punishment of intellectual property violations,[37] and multiple attempts to develop international agreements (such as ACTA).[38]

Locations of Control: The Role of Private Intermediaries

If we look a bit more closely at the three areas discussed above—surveillance, content restrictions, and intellectual property enforcement—we can identify a shift in the location of policymaking and control. Starting again with the issue of surveillance, the crucial

[33] Yochai Benkler, *The Wealth of Networks: How Social Production Transforms Markets and Freedom* (Yale University Press 2006); Lawrence Lessig, *Remix: Making Art and Commerce Thrive in the Hybrid Economy* (Bloomsbury 2008).

[34] Milton Mueller, *Networks and States: The Global Politics of Internet Governance* (MIT Press 2010) 131.

[35] James Boyle, 'The Second Enclosure Movement and the Construction of the Public Domain' (2003) 66(1) Law and Contemporary Problems 33.

[36] Christopher May, 'Globalizing the Logic of Openness: Open Source Software and the Global Governance of Intellectual Property' in Andrew Chadwick and Philip N Howard (eds), *The Routledge Handbook of Internet Politics* (Routledge 2009).

[37] See Robert Klotz, *The Politics of Internet Communication* (Rowman & Littlefield 2004).

[38] Michael Geist, 'The Trouble with the Anti-Counterfeiting Trade Agreement (ACTA)' (2010) 30(2) SAIS Review 137.

role of internet companies in the monitoring of citizens and user behaviour was highlighted drastically in programmes such as Prism which were revealed by Edward Snowden. With their business models based on collecting and analysing user data, these companies have generated and stored detailed information about a growing number of people worldwide, including their locations, activities, preferences, friends and social networks, and sometimes political orientations. 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. While those arguing for the expansion of mass surveillance (such as the new Director of GCHQ, Robert Hannigan) have criticized internet companies for failing to address cybercrime and to allow governments to monitor their services,[39] others have analysed the close and friendly relations between government and companies such as Google which suggest cooperative and supportive interactions between both forces.[40]

Even before Snowden, reports such as the Google *Transparency Report* specified some of the more official ways in which governments use social media to collect information about its users. Between July and December 2013, Google received requests for the data of over 18,000 users in the US, and over 3,000 users in the UK (which is, in the case of the US, requests for 3,000 different users a month, or 100 different users each day).[41]

Activists and dissidents that are targeted by governmental surveillance have experienced how their use of social media platforms and digital communication tools can put both their activities and their health and lives at risk. As one of the first so-called 'social media revolutions', the 'Green Revolution' in Iran in 2009 demonstrated how social media platforms like Twitter and

[39] Ben Quinn, James Ball and Dominic Rushe, 'GCHQ Chief Accuses US Tech Giants of becoming Terrorists' Networks of Choice' (*The Guardian*, 3 November 2014) <www.theguardian.com/uk-news/2014/nov/03/privacy-gchq-spying-robert-hannigan> accessed 3 December 2014.

[40] Julian Assange, *When Google Met WikiLeaks* (OR Books 2014)

[41] Google, 'Transparency Report 2014' (*Google*, 2014) <www.google.co.uk/transparencyreport> accessed 3 December 2014.

YouTube could help mobilize the public and spread information internationally, but also serve as a means to identify protesters. As Hofheinz notes: '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'.[42] In Iran, Tunisia and elsewhere, authorities used Facebook to scrape user data. In Syria, opposition supporters that used social media were targeted through malware that installed spying software onto the infected computer, for example to capture webcam activity, and stole YouTube and Facebook login credentials.[43] State reactions to the London riots in the UK in August 2011 mirrored some of these responses as protesters were identified through their use of social networking, and merely communicating about the riots on social media led to severe punishment, including prison sentences.[44]

As the collection and storage of data is outsourced to social media companies, telecommunications services and ISPs, so is the targeted intrusion, monitoring and analysis of user data. Companies such as Finfisher and Blue Coat provide sophisticated tools for surveillance and filtering to governments around the world, including both Western democracies and authoritarian states.[45]

While the surveillance theme points to the use of intermediaries by the state, the second area—content restrictions—unveils more direct

---

[42] Albrecht Hofheinz, 'Nextopia? Beyond Revolution 2.0' (2011) 5 International Journal of Communication 1417, 1420.

[43] Nart Villeneuve, 'Fake Skype Encryption Software Cloaks DarkComet Trojan' (*Trend Micro Malware Blog*, 20 April 2012) <http://blog.trendmicro.com/fake-skype-encryption-software-cloaks-darkcomet-trojan/> accessed 3 December 2014.

[44] Owen Bowcott, Helen Carter and Helen Clifton, 'Facebook Riot Calls Earn Men Four-Year Jail Terms amid Sentencing Outcry' (*The Guardian*, 16 August 2011) <www.guardian.co.uk/uk/2011/aug/16/facebook-riot-calls-men-jailed> accessed 3 December 2014.

[45] Morgan Marquis-Boire and others, 'Planet Blue Coat: Mapping Global Censorship and Surveillance Tools' (*The Citizen Lab*, January 2013) <https://citizenlab.org/wp-content/uploads/2013/01/Planet-Blue-Coat.pdf> accessed 3 December 2014; Morgan Marquis-Boire and others, 'For Their Eyes Only: The Commercialisation of Digital Spying' (*The Citizen Lab*, 2013) <https://citizenlab.org/storage/finfisher/final/fortheireyesonly.pdf> accessed 3 December 2014.

interventions by the private sector. Beyond the classic forms of state-sanctioned censorship and law-based content limitations, app stores and social media platforms have created their own rules and practices for accepting and rejecting content. Apple, for example, 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.[46] Facebook has taken down activist pages in the run-up to protest events as well as dissident pages such as 'Anarchist Memes', a page dedicated to anti-capitalist, anti-racist and feminist rights, 'as part of a growing effort by Facebook to crack down on the presence of political groups on its network'.[47] It has also censored cartoons and other content, such as pictures of breastfeeding mothers because of alleged 'indecency'.[48] The company thereby makes decisions with severe political and human rights implications. It has thus become a 'social media police force'[49] that is bound by its own terms of service, cultural background and political leanings, rather than the rule of law. It has joined other intermediaries such as ISPs and search engines as 'proxy censors'.[50]

Such intermediaries also encompass providers of other relevant infrastructure, including server space, domain registration, and funding. In December 2010, Amazon, PayPal and others demonstrated their crucial gatekeeping role when they closed the services they had previously provided for WikiLeaks, depriving the leaks platform of its domain name and of access to necessary funds in the middle of a major release (the Cablegate leaks). This 'denial of

[46] Christina Bonnington and Spencer Ackerman, 'Apple Rejects App that Tracks U.S. Drone Strikes' (*Wired*, 30 August 2012) <www.wired.com/2012/08/drone-app> accessed 3 December 2014.

[47] Lina Dencik, 'Why Facebook Censorship Matters' (*JOMEC Blog*, 13 January 2014) <www.jomec.co.uk/blog/why-facebook-censorship-matters> accessed 3 December 2014.

[48] Ben Norton, 'Fascist Facebook? The Social Network Giant's Double Standards' (*Counterpunch*, 10 January 2014) <www.counterpunch.org/2014/01/10/fascist-facebook> accessed 3 December 2104.

[49] Dencik (n 47).

[50] Seth F Kreimer, 'Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link' (2006) 155(11) University of Pennsylvania Law Review 11, 13.

service'[51] propelled the providers of critical services into the spotlight of the debate around WikiLeaks and freedom of expression. It 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, the actions by Amazon, PayPal, etc., highlighted the vulnerability of these services to political interventions, as they coincided with pressure from members of the US political elite, both inside and outside government.[52]

Finally, the fight against filesharing and remixing offers particularly useful insights into the outsourcing of policy. The typical chain of action would see a property owner or their representative, such as the Recording Industry Association of America (RIAA), commission a law firm as an intermediary which would then contact the ISP or content provider and request the latter to take down particular content or a link. Such interactions between private firms have led to requests to remove, on average, 20-25 million URLs from Google searches each month, by summer 2014.[53] Similarly, the US Copyright Alert System was established in 2013 as an agreement between the copyright holder industry and ISPs in which copyright holders identify shared copyrighted material and ISPs exert punishment by warning the respective customer or, as a last resort, cancelling their internet connection. The mechanism bypasses governmental and judicial oversight and puts both the definition of, and the punishment for, copyright infringement in the hands of content owners and ISPs.[54] According to Mueller, 'the regulatory trend that constantly emerges from the [intellectual property] tension is a shift of the responsibility for monitoring and policing Internet conduct

[51] Yochai Benkler, 'A Free Irresponsible Press: WikiLeaks and the Battle over the Soul of the Networked Fourth Estate' (Working draft 2011) <www.benkler.org/Benkler_Wikileaks_current.pdf> accessed 3 December 2014.

[52] ibid.

[53] Google (n 41).

[54] Sean Flaim, 'Op-ed: Imminent "Six Strikes" Copyright Alert System Needs Antitrust Scrutiny' (*Ars Technica*, April 2012) <http://arstechnica.com/tech-policy/news/2012/03/op-ed-imminent-six-strikes-copyright-alert-system-needs-antitrust-scrutiny.ars> accessed 3 December 2014.

onto strategically positioned private sector intermediaries'.[55] 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.

Opposing Internet Restrictions and Surveillance

The trend towards the limitation of internet freedoms and to pervasive surveillance is heavily contested and has led to growing campaigns for digital rights as well as protests against restrictive internet policies. The surveillance scandal revealed by Edward Snowden has triggered street protests and international campaigns such as 'Stop Watching Us'.[56] Protests have been complemented by other campaign strategies, e.g. petitions[57] and litigation.[58] That such mobilizations can have significant success was demonstrated earlier by the protests against the 'Stop Online Piracy Act' (SOPA), a US bill to combat online copyright infringement. A 'transnational coalition of engineers, academics, hackers, technology companies, bloggers, consumers, activists, and Internet users'[59] managed to defeat the bill in a 'David and Goliath story in which relatively weak activists were able to achieve surprising success against the strong'.[60] Larger organizations that advocate for digital rights, such as the Association for Progressive Communications (APC), have brought their concerns

[55] Milton L Mueller, *Networks and States: The Global Politics of Internet Governance* (MIT Press 2010) 149.

[56] <https://rally.stopwatching.us> accessed 3 December 2014.

[57] <https://necessaryandproportionate.org> accessed 3 December 2014.

[58] The Open Rights Group and other organizations challenged the UK surveillance regime by taking the UK government to the European Court of Human Rights, see Matthew Taylor and Nick Hopkins, 'GCHQ faces legal challenge in European court over online privacy' (*The Guardian*, 3 October 2013) <www.theguardian.com/uk-news/2013/oct/03/gchq-legal-challenge-europe-privacy-surveillance?CMP=twt_gu> accessed 3 December 2014.

[59] Susan K Sell, 'The Revenge of the "Nerds": Collective Action against Intellectual Property Maximalism in the Global Information Age' (2013) 15(1) International Studies Review 67, 67.

[60] ibid 68.

to debates at international institutions and have participated in multi-stakeholder fora such as the Internet Governance Forum and the Internet Corporation for Assigned Names and Numbers.

Yet these strategies have been complemented by other forms of intervention, such as the development of technological alternatives and encryption tools, and by changes in individual communication practises. Responses to the surveillance scandal have included the increased use of anonymization tools, such as PGP and TOR, and their promotion through 'Cryptoparties'. Non-profit activist-based internet services such as Riseup.net have offered secure email accounts, mailing lists and online spaces such as blog and pad platforms, and have collaborated with similar groups across the globe to create networks of activist communication that are less prone to censorship and surveillance. Efforts to create alternative forms of social networking, such as Lorea.org, have added to a strategy that focuses on the development of autonomous and civil society-based media infrastructure. This approach is informed by the individualism of cyberpolitics which emphasizes the right of the individual to explore all information in cyberspace—unimpeded and uncensored—and to contribute and share knowledge.[61] It also draws from the rather loose and often temporary forms of association and 'connective action'[62] that online activists and other 'netizens' have developed and experimented with, and that have moved beyond established formats such as unions, parties, and formal civil society organizations.

Rather than advocating for policy change, many internet activists thus see their job as creating 'self-managed infrastructures that work regardless of "their" regulation, laws or any other form of governance'.[63] They operate 'beyond' the classic divisions of social movement activism in 'insider' and 'outsider' approaches, i.e. in

[61] Tim Jordan, *Cyberpower: The Culture and Politics of Cyberspace and the Internet* (Routledge 1999).

[62] W Lance Bennett and Alexandra Segerberg, *The Logic of Connective Action: Digital Media and the Personalization of Contentious Politics* (Cambridge University Press 2013).

[63] Indymedia activist, cited in Hintz and Milan, 'At the Margins of Internet Governance' (n 10) 31.

collaborative and participatory advocacy versus protest and disruption. Instead, they build alternatives to existing communication infrastructure and seek to bypass laws and policy obstacles. Their strategies focus on prefigurative action, rather than attempts to influence policy processes they regard as dominated by existing powers.[64] In their efforts, they thus mirror privatized 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.

At the intersection of policy advocacy and prefigurative action, new strategies of grassroots do-it-yourself policy-making and 'policy hacking' are emerging that focus on developing new model laws and regulatory proposals, rather than merely advocating for them. Often this has involved digital tools to crowd-source contributions from a wider range of civil society. Policy hacking and DIY policy-making has extended from the local level (e.g. the making of a new transparency law in the city of Hamburg in 2012) to the national (e.g. the Icelandic Modern Media Initiative which created proposals for new media laws in Iceland) to the international (e.g. the development of a model law on net neutrality at the Internet Governance Forum).[65] Here, the 'outsourcing' of policy-making has involved civil society actors who have taken legislative development into their own hands.

Conclusion

Internet policy in the (not anymore so) new millennium has changed as both the private and state sectors have strengthened their grip on technical infrastructure and its uses. The deterritorialized spheres of the internet have partly been reterritorialized by states; the practice of filtering and blocking content is expanding; information and ideas

[64] Arne Hintz and Stefania Milan, 'Networked Collective Action and the Institutionalised Policy Debate: Bringing Cyberactivism to the Policy Arena?' (2013) 5(1) Policy & Internet 7.

[65] Arne Hintz, 'Policy Hacking: Citizen-based Policymaking and Media Reform' in Des Freedman and Robert W McChesney (eds), *Strategies for Media Reform: International Perspectives* (Fordham University Press 2015, forthcoming).

are being commodified; and digital surveillance has become pervasive. Thus the 'policies of liberation' which early cyberspace and cyberlaw thinkers had envisioned are giving way to 'policies of control'.[66]

However we can observe another trend which intersects with this development—the privatization of internet policy. Commercial intermediaries are enlisted to police the net and develop new rules for allowing as well as restricting communication practices and freedom of expression. They are required by governments to monitor their users and store data exchanges, but they also collaborate to define and punish objectionable user behaviour, and they implement their own rules to provide, and withdraw, vital spaces and resources for communication. Responsibility and authority for policy-making and implementation are thus shifting to the private sector in the shape of ISPs, telecommunications services, social media platforms and other providers of online services.

Resistance to problematic policies and practices that are implemented in this way—from surveillance to content restrictions—is equally transitioning from a state focus to prefigurative action by civil society groups. Established forms of advocacy and campaigning are complemented with the development of alternative platforms, tools for circumvention, and model laws and regulations. Demands for privacy, free expression, an open internet and unrestricted exchange of knowledge are thus not just raised through protest and lobbying but through the self-organized creation of technological as well as policy alternatives that embody and implement these values. The contestations over current issues such as surveillance take place increasingly in the arena of private, non-state media actors and infrastructures.

[66] Katharine Sarikakis, 'Mapping the Ideologies of Internet Policy' in Katharine Sarikakis and Daya K Thussu (eds), *Ideologies of the Internet* (Hampton Press 2006) 171.