Original Research Article

BIG DATA & SOCIETY

Big Data & Society
January–June 2015: 1–14
© The Author(s) 2015
DOI: 10.1177/2053951715580599
bds.sagepub.com
SAGE

'Hacking multitude' and Big Data: Some insights from the Turkish 'digital coup'

Paolo Cardullo

Abstract

The paper presents my first findings and reflections on how ordinary people may opportunistically and unpredictably respond to Internet censorship and tracking. I try to capture this process with the concept of 'hacking multitude'. Working on a case study of the Turkish government's block of the social media platform Twitter (March 2014), I argue that during systemic data choke-points, a multitude of users might acquire a certain degree of reflexivity over ubiquitous software of advanced techno-capitalism. Resisting naïve parallels between urban streets and virtual global streets, the article draws on Fuller's 'media ecologies' to make sense of complex and dynamic interactions between processes and materialities, strategies of communication and mundane practices. Such a dense space is mostly invisible to network and traffic analysis, although it comes alive under the magnifying lens of digital ethnography. As the Turkish government tried to stop protesters on both the urban and the Twitter spheres, alternative material configurations and new hybrid formations and practices emerged. I try to bring this process alive following the traces – that is, a combination of digital data and materialities – of a social space between the protest for Twitter access, the 'digital coup' and the interactions that this situation determined. In the final section, I briefly explore two research trajectories which can further develop my initial formulation of a 'hacking multitude'. I argue that a generalisation of hacking/multitude is problematic for the political, cultural or economic processes more directly associated with Big Data.

Keywords

Big Data, hackers, multitude, Internet, Twitter, digital ethnography

> The Net interprets censorship as damage and routes around it. (Jon Gilmore, founder of the Electronic Frontier Foundation)

Con-text

Ten days before Turkish local elections, on 20 March 2014, PM Tayyip Erdogan blocked access to Twitter: allegations of Erdogan's corruption had circulated on the social media platform, receiving little notice outside Turkey. This dramatically changed when they eventually tried to stop people from tweeting altogether. Mr Erdogan firstly deployed a well-known discourse around social media as 'bad', since they can corrupt people's morality.[1] This is a strategy of placing media outside the sacred sphere: social media in particular, with their inherently global audience, resemble a foreign invasion tearing apart the fabric of society.[2]

> The blockage on Twitter began [at] circa 11 pm. All of a sudden users started to talk about how some of their friends couldn't log in on Twitter. After a couple [of] hours I also couldn't log in, so I followed the news on my Facebook timeline. (Online interview)

Goldsmiths, CUCR, University of London, London, UK

Corresponding author:
Paolo Cardullo, Goldsmiths, CUCR, University of London, Laurie Grove Bath, London SE14 6NW, UK.
Email: p.cardullo@gold.ac.uk

Despite the block imposed on Twitter, hashtags concerning Turkey censorship started to trend from the next day, so attracting more users: tweets and unblocked social media increasingly showcased alternative workarounds, initiating a 'hacking game' which I follow below.

The paper narrates this Internet censorship attempt and its circumvention, following two main leads. Drawing from diverse data points, I first suggest that the combination of denial of service, social media practices and hackers' intervention started a learning curve in people being affected by the ban. A certain degree of users' reflexivity and the resulting repository of technological expertise are crucial to the workings of a 'hacking multitude'. In the first instance, 'multitude' is intended as a mass of ordinary Internet users whose daily media practices, *opportunistically and unpredictably*, are means of digital and informational production (Virno, 2003).

The second reflection this paper wants to start is around the implications that a potential generalization of hacking practices might have for the political, cultural or economic processes more directly associated with Big Data. My initial findings show that new social and material assemblages started producing data over and *beyond* Twitter. I will foreground traces of this generative social space which, I contend, is made invisible in the Big Data flow.

In order to grasp the complexity of this emerging media system, which has not a single entity responsible for it nor is it simply imposed from above, I draw on Fuller's reworking of the term 'ecology': a 'massive and dynamic interrelation of processes and objects, beings and things, patterns and matter' (Fuller, 2005: 2). To understand the multi-layered, non-linear, unfolding of media ecologies, Fuller suggests attending to the liveness of the event, to participate in the interactions of these systems 'with no control sample'. Partly, the events narrated here are an attempt to bring this process alive. The story unfolds using tweets and photographs as they became available on Twitter during a massive stand against censorship, which I followed throughout. My narrative juxtaposes moments of mediatic synthesis, made of Big Data configurations, and some 'basic practices of how people construct the social and cultural world' (Couldry, 2012: 137). These practices are generally hidden in aggregate statistics, but they become more intense under the magnifying lens of digital ethnography.

In the second part of the paper, I integrate online data with online interviews of Turkish Twitter users. I haven't been directly involved in the observation of the Turkish protests from the streets.[3] However, I managed to reach some protagonists of the events I narrate, thanks to intense snowballing, following and negotiations on the terms of our online interaction (e.g. encrypted conversations), through specific mailing lists, social media and forums. These interviews therefore contain for me a wealth of details and perspectives from the 'field'.[4]

In the end, I develop the concept of a 'hacking multitude'. I argue that basic practices of hackerdom and their potential recurrence in the economies of digital information can become, at least temporarily, crucial elements in the architecture of the Internet. Ultimately, they can change the morphology of data itself. In so doing, a social process of collaboration, learning and reflexivity starts appearing, at least with regard to contestation of Internet access.

This article focuses on Turkey because, differently from many other countries that experienced the so-called 'Web 2.0 Revolutions', it has a potential critical mass of users where digital devices and social media platforms are part of many people's everyday life. Turkey ranks 4th in number of Facebook members and 11th in terms of Twitter users: the exponential increase in social media users is also due to traditional media being heavily centralised and censored (Furman, forthcoming). Twitter became popular in Turkey on the wave of #OccupyGeziPark uprising:

> TV and other media did not cover the events: mobile phones became the TV, photos were published on Twitter and other websites. Citizen journalism became the de facto news agency for all. (Online interview)

Much has been written on the connections between social media and recent street protests. Castells suggests that the Internet creates protests. Speaking about a tradition of 'techno-euphoria and techno-determinism' (Fuchs, 2013), he argues that the Internet is 'a necessary though not sufficient component… decisive to social movements' (2012, in Fuchs, 2013: 84). In Twitter, some see an instrument essential for designing the *choreography of the assembly* during street protests (Gerbaudo, 2012), and generally being an effective *megaphone* (Murthy, 2013). Developing a politics of *presence* in the global city, Georgiou (2013: 142) suggests that for marginal groups 'the physical space of the city is no longer enough. The urban street is revived and extended to the global mediated street'. A large-scale research on the 2011 London riots, 'Reading the Riots', however, found that there was no significant evidence of Twitter being central to the organisation of the riots. Despite the moral panic around social media that the events sparked, their analysis of over 2.5 million tweets shows that the popular platform was rather used to organise post-riot clean-up operations.[5] Social media are not the cause of protests, Fuchs (2013: 204) concludes, rather a 'mirror of the power structures we find in society'.

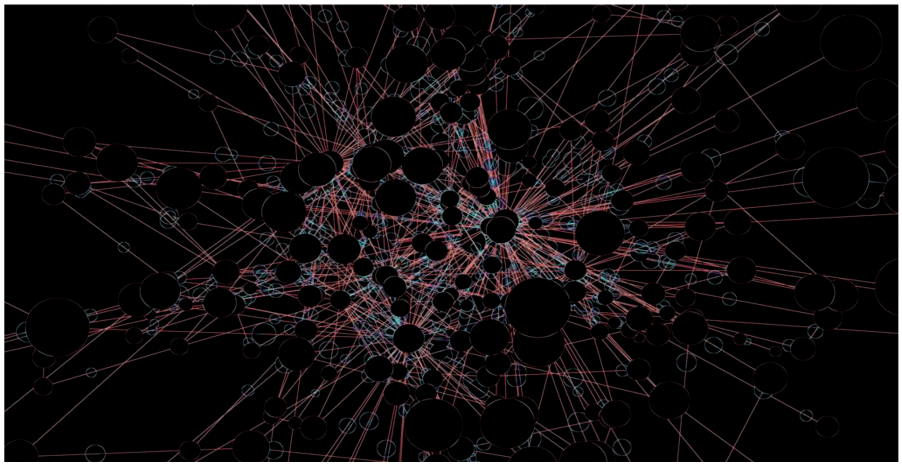
An evaluation of the effects of digital insurgency on the Turkish political landscape is beyond the scope of this paper. There are, however, some open questions, particularly during transformative moments, around how data is made manifest to us and the processes that make this data possible. How is the morphology of digital data being changed by the evolving political landscape? To what extent can a generalised form of digital disobedience effectively change the consistency and relevance of Big Data, such as Twitter traffic analysis or grouping by hashtag? Moreover, what configurations would users form in relation to their online privacy and their right to use the Internet in a scenario of state surveillance? What kind of social alliances are forged during circumvention of Internet censorship? According to De Landa, our 'mathematical technology' was always incapable of modelling self-organising phenomena: 'non-linearities were eliminated as much as possible from mathematical models, making non-linear effects like chaos "invisible"' (De Landa in Crary and Kwinter, 1992: 133). An analysis of multiple data points, such as tweets, photographs and interviews, rather allows the fine grain of a social process, which the very notion of 'data flow' hides, to come alive.

Governments, such as Egypt, China or Pakistan, generally have had good or modest results in implementing Internet censorship (Deibert, 2009, 2012), but its impact on protests is ultimately uncertain. Censorship attempts are incomplete and evolving too: in Turkey, for instance, tougher measures are now being introduced, involving controversial spying software and more centralised administration of the Internet.[6] There are more dedicated studies on this matter (e.g. Deibert, 2009, 2012), but I want to flag up governments' adoption of paid 'trolls' in order to shift public opinion on social media.[7] In my view, this is a sign that censorship and filtering alone, although on a massive scale, cannot address the full dynamism of media ecologies of digital communication. Governments too need media practices, they need to play on the same ground of, and in fact they hack, the 'hacking multitude'.

Materialities

I will now start unfolding the ecology around the 'digital coup'. This is made of institutional constraints, which I sketched in the introductory section, Big Data representations, discussed in the next section, and materialities. A focus on materialities – as both media practices and physical infrastructures – not only demonstrates that data does not simply flow at a push of a button but also shows how social space comes alive in the choke-points of such a 'flow'.

Initially, the Twitter ban in Turkey was a simple block at domain level. Domain Name Service (DNS) is a distributed and hierarchical system which translates human readable hostnames (www.twitter.com) into the numeric IP address required to resolve that request (for instance, 204.71.177.71).[8] DNS is a sort of phone book of the Internet, which indexes IP addresses for website. Unlike a phone book, DNS can be quickly updated, allowing a service's location on the network to change without affecting end users, who continue to use the same host name. DNS is organised in a hierarchical fashion with 13 very powerful root name servers at the top level. 'Copies' of these super-servers are distributed worldwide via a network addressing and routing methodology which sends requests to the topologically nearest node in a group of potential receivers. This has accelerated a decentralised service, with the deployment of *physical* (rather than logical) root-servers outside the US: for example,



OpenDNS is a distributed service over geographically dispersed servers, claiming a 'self-healing network across three continents' (OpenDNS.com).

'Self-healing' is a relevant concept here. If any regional server is affected by outage or block, the whole traffic can be re-routed to the nearest (physical) location. In this configuration, the Internet is typically represented as a complex 'network of networks':

> The block was simply directing users to a web page which said 'Twitter is banned via jurisdiction', which was not. Telecom companies adjusted their DNS servers in order to advertise that page as Twitter. Many people switched DNS servers. (Online interview)

This simple geopolitics of the Internet reminds us of Castells' vision. The network is seen from the perspective of nodes and set in the context of online freedom from 'attacks', malware software or censorships. However, Castells' configuration 'leaves unresolved the relative causal weight of *everyday context* versus operations of networks or *people's positioning* within networks' (Couldry, 2012: 115, emphases added).

Material practices and non-humans are constitutive parts of Internet ecologies. They produce digital data via their relentless labour. They are the network too, part of the everyday context in which networks operate. I will discuss practices in the second part of the paper, with lots of details and stories that came out from my online interviews with some Turkish tweeps. Materials make the main argument of this section: a physical architecture of the Net starts to appear. This has been unveiled by the very block that meant to make it unavailable to the wider public in the first place.

Observers' eyes were by now set on any statistical indicators that could capture what was going on in Turkey: How successful was the block? Did traffic reveal an adequate response from users?

Big numbers

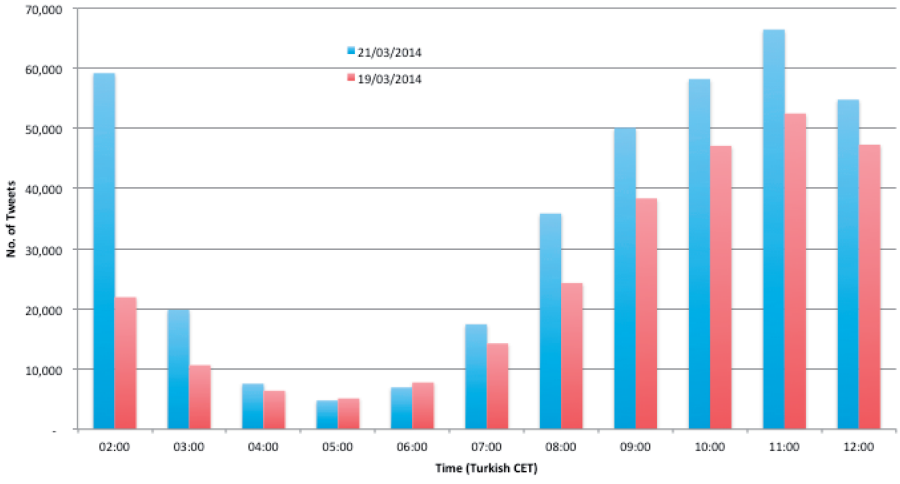
I now discuss some metrics around the popularity of Twitter in Turkey and around Twitter hashtags that were trending during the 'digital coup'.[9] I present below two groups of quantitative indicators, as they became available during the period of observation.

1. Hours after the attempt at blocking Twitter, news grew under the headline/hashtag: #Twitteris BlockedinTurkey, and similar. The infographic below was circulated over 4000 times (considering only direct re-tweets) on the same day Occupy Wall Street NYC produced it.

Part of the online world seemed to identify themselves with Twitter users being blocked in Turkey, while Turkish users became aware of being 'trending' on the platform. Infographics' powerful message is to

sample and aggregate large swathes of users and to make representations speak for an imagined community of people. They are not just aesthetically appealing forms of visualisation of often dry data. Digital communication fabricates data, but data enacts 'people'. It creates instances of ontological consistency of a subject (Ruppert, 2011). In this sense, hashtags are powerful forms of aggregation, although they are rather weak for measuring belonging. The crucial thing is that Twitter transforms grouping by hashtags into 'trends', by the way of publishing metrics on their popularity. Trend is per se a piece of information insomuch as it circulates on more traditional media, which monitor Twitter metrics as an approximation of the interest in a certain subject. Communication therefore becomes data, which is turned into information: a circular repetition of the same.

2. Traffic analysis from diverse sources suggested that restrictions had failed to stop digital insurgency against censorship. Mikko Hypponen, Chief Researcher at F-Secure,[10] shared a graph which shows an increase of 138% on the volume of tweets from Turkey in the immediate hours after the ban: this is equivalent to 'some 17,000 tweets every minute'.[11]



Looking at some indirect indicators, there are reasons to believe that a vast part of the contribution to the trend on the social platform was coming from Turkey itself. Twitter's popularity in Turkey is generally very high. Turkish is ranked as the eighth language spoken on the social media platform, accounting for the 2% of all tweets exchanged globally (Leetaru et al., 2013); the Turkish president, Abdullah Gul, who famously tweeted after the ban imposed by his government, is ranked third in the league of Twitter followers among world leaders (with a staggering 4.2 million followers)[12]; with a percentage of Twitter users higher than the US (79% vs. 73%), Turkish tweeps are at the top of the world chart.[13]

Despite providing a useful entry point in the discussion of online censorship, traffic analysis does not reveal the complexities of how data is generated in transformative moments. Big Data analysis gives the impression that measures to circumvent the block had spread fast, reflecting a more generalised political opposition in Turkey. My contention is that new social and material assemblages were conditioning – and were in turn conditioned by – this new data flow, in a dialectical and non-linear manner. While the paper does not specifically investigate what this meant for Turkish society and its changing political landscape, it attempts to foreground traces of this generative social space made invisible in aggregate analysis.

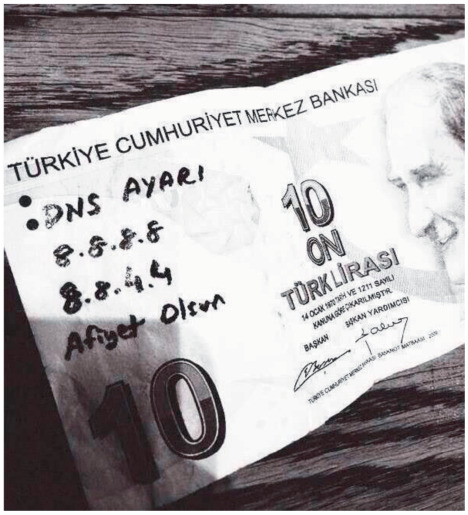
Small numbers

In order to capture this emerging process, we need to equip ourselves with other tools. I first build on my direct engagement as an active tweep during the events I narrate here. Drawing on the anthropological scholarship emerging in response to the Internet (Hine, 2000, 2013; Underberg, 2013), I use digital ethnography with discourse/content analysis of: tweets, photographs circulated on the platform, and links included in tweets (few thousands overall). I then circulated my research blurb on mailing lists and social networks, managing to interview some Turkish Twitter users who actively took part in the events.[14] These interviews are therefore direct accounts from the 'field', the social space between the Turkish block of Twitter and users' attempts to circumvent such censorship.

'Digital ethnography' is here intended as a method with multiple data points to allow for immersion in

the experience of another culture (Underberg, 2013), a protest culture in this case. Digital ethnographers' toolkit to study the Internet evolves with every setting, kind of data, subject and site, as these become available or useful to her: 'Unlike big data studies which often aggregate data across single platforms, ethnography can explore how events in one place are made meaningful, in surprising and contingent ways, in another' (Hine, 2013). While digital ethnography helps the researcher to connect with the 'field' under observation, sociological discourse analysis allows imagination and reciprocity between otherwise seemingly distinct realities, the virtual and the actual. Discourse analysis in digital ethnography explores the way in which accounts are made convincing while maintaining the critical distance of the ethnographer. At the same time, 'the analyst presents herself as a competent cultural member', adding validity to the set of data collected (Hine, 2000: 143).

The relation between what appears to happen online – increasingly conveyed by Big Data metrics (number of followers, friends, likes, shares, etc.) – and how social life is constructed everyday – undeniable domain of ethnographic tradition – is a tricky balance in digital ethnography. It requires attending to both detailed online observation and to the awareness that most of this material is already present as digital data. In the next section, I try to foreground the social space around the Twitter ban. This 'social' emerges in a contingent process of Internet surveillance from a nation state and spreads through streets and digital media, in the context of daily engagement with communication technology, production of digital data and political opposition.



Re-text

By now, the problem became how to communicate alternative DNS numbers and instructions to Turkish people who were unable to connect to Twitter in the first place.

> The info [about DNS] was **all over Facebook** and even the mainstream newspapers had articles that would give guidelines.
>
> **The word** [about VPN] got around fast on the day Twitter was blocked. Facebook posts were already circulating beforehand.
>
> My friends and colleagues asked me if I could access YouTube and/or Google, and also how to do it. I helped them to change settings. The advice rapidly spread far and wide **via friend-to-friend** network.
>
> **One [of] my colleagues** sent an email about a simple guide for using VPN and proxies. (Online interviews)

These extracts foreground a vernacular element of proximity in experiencing a global network: friends, colleagues, word-of-mouth and face-to-face interactions. Importantly, workarounds were also repeated on physical walls and other material objects. Their message was in the form of an alpha-numeric string, such as the now ubiquitous 8.8.8.8, Google DNS sequence.

> Google DNS servers were written on walls and leaflets. (Online interview)
>
> Q: How wide spread was the attempt to reconnect to Twitter? A: It was very widespread, everyone wanted to do it, even my mum. People were putting DNS numbers on their windows. (Skype interview)

This is when part of Turkey seemed to familiarise themselves with the rules of a game few had thought they needed to play: only one of my interviewees had tried to circumvent censorship during a previous YouTube ban. Crucially, they all say that they will *definitely* do the same in future.

Photographs that circulated on Twitter help to render this climate of growing awareness around Internet freedom.

It is a contention of visual sociology scholars that photographs give texture to place and help to strengthen arguments (Knowles and Sweetman, 2004). Maybe because they carry and reproduce a reservoir of affective responses (Terranova, 2004). They are compressed, edited, aligned with text, they irremediably become 'poor images': 'The poor image is a copy in motion. Its quality is bad, its resolution substandard. As it accelerates, it deteriorates' (Steyerl, 2009). Large numbers of photographs started circulating on Twitter and other media, becoming a phenomenon in itself. Photographs are digital data too, a combination of

pixels and bits. They, however, need to be emphasised, since they disappear from view when aggregated in trending hashtags. Photographs are important because they evoke context: specific people, places or events. They provide a sort of 'existence proof', a reminder of people in 'flesh and blood' (Becker, 2002). I would argue that this material dimension is somehow lost in Big Data analysis.

I selected some photographs from the usual deluge of Twitter data, while following live the 'digital coup' in Turkey. They are presented here as episodic vignettes, exactly like ethnographers would use extracts of long interviews, or a network analyst would isolate particular tweets out of thousands. Triangulated with other data, they will hopefully give the reader a heuristic grasp on this composite scenario: a banknote, 10 Turkish Liras, with the Google alpha-numeric inscription; a restaurant menu outside an al-fresco patio, with iPhone and Google DNS instructions; a few citizens gathering around a poster which explains how to re-connect to Twitter.

I find this latest photo particularly helpful in revealing what a 'hacking multitude' might be and how it might operate. This is for three reasons.[15] First, the photograph speaks of a localised protest, in Istanbul here and now: it immediately gives the *context*, which photography can so effectively evoke. Second, it recalls the *experience* of Internet censorship, its affective dimension. Notes written on walls, such as directives or instructions, convey the state of emergency proper of transformative moments. There is here a sense of suspension: we do not know what exactly these people are going to do with their

new workaround, whether they will be able to successfully activate it for their own purposes, or if they are already spreading the news to others. In other words, this image recalls 'wirelessness', 'an experience trending toward engagement with things, objects, gadgets, infrastructures and services, and imbued with indistinct sensations and practices of network-associated change' (Mackenzie, 2011: 5). Importantly, 'wirelessness' is not a pure sensation of transition through digital networks and devices, a flow at a push of a button, but an experience made of attempts, errors and repetitions (Mackenzie, 2008). I would argue that in moments of suspension between actions and networks, the multitude's reflexivity and its potential for social interactions might be set in motion. Its inherent virtuality is a relevant concept: it is in the nature of a multitude to unpredictably respond to an evolving situation (see Virno, 2003).

Finally, the photograph reminds us of the *ordinariness* of the Internet. By-standers here look like ordinary people: frankly, quite boring compared to mainstream representations of hackerdom (e.g. the terrifying Anonymous). They appear intent at modifying their communication tools, ordinary mobile phones ('ordinary' as used by Raymond Williams, as for mundane, vernacular, 'of the people'). This is crucial for understanding what a 'multitudo' is. Its Latin root 'multis', which we translate in English as 'many', mistakenly points to a vast number of people. If that was the case, we would circularly fall into a Big Data logic: the more data comes, the more truthful data appears to be. Rather, I use multitude as 'mob', 'rabble' or 'throng', that is an indistinct and unclassifiable group of individuals.[16]

After failing to adopt pressure directly on Twitter, which appeared to stand for the 'freedom of speech',[17] the Turkish government managed to block requests negotiated via Google-owned or any other public DNS. Similar to what happens in China,[18] they heightened the level of censorship, moving the block to IP level. There are few ways of doing this, but such a discussion is beyond the scope of this article. The important thing is that public DNS was now not effective, because no Internet Service Provider in Turkey could reach Twitter by IP address any longer. When Turkey managed to block Twitter at IP level, more articulated responses became necessary in order to avoid the ban. Crucially, these had to be learned.

> VPN time! (tweet)

The hacking game

I will now briefly explain the functioning of VPN and TOR, emphasising first their popularity and then social aspects around their implementation.

Virtual Private Network means that a user can securely connect to a computer by using a technique called 'tunnelling'. The VPN client communicates over the public Internet and sends the computer traffic through an encrypted connection to a VPN server. Using this connection, VPN customers can securely access the Internet from their remote device, bypassing any filtering included in their Internet Service Provider's policy. VPNs are usually offered as a pay-per service, so trust is regulated by the terms of provision of such a service. Therefore, there are a few drawbacks in this method: reliance on private traffic, difficulties in setting up secure client–server connections and security flaws (e.g. institutional controls on the provider).

TOR, The Onion Router, is both a free software and an open network that help users stay anonymous and defend themselves against traffic analysis.[19] TOR bounces signal *at least* three times in several *random* relays, to make it anonymous. For efficiency, TOR uses the same circuit for *no longer* than 10 minutes.[20] Moreover, each hop in the network exchanges an encryption, or 'onion skin', around the original transmission. TOR is not just an application, but an ever-changing network of proxies, made of random relay servers and strong encryptions. It provides a continuum in which the degree of privacy is generally a 'function of the number of participating routers versus the number of compromised or malicious routers' (Wikipedia).[21]

TOR shreds to pieces the idea that the Net is controllable in any single nation. It is not secure, but it is anonymous. VPN is not anonymous, but it is probably more secure (if you trust the service provider). To put it bluntly, while VPN is a solution favoured by business (it is a paid-for service, after all), TOR is the obvious choice of 'hackers' (it is Free and Open Source, in fact). Most of my interviewees had embraced VPN as their favourite method for going online, and they generally reported a hassle-free experience. Importantly, none of them had ever used such tools before.

> I decided to download VPN Unlimited on my Android phone. It was easy to operate and didn't seem to cause too much speed or reliability issues.
>
> Actually it was pretty easy. Through my friends' advices I downloaded two VPN applications to my mobile phone. (online interviews)

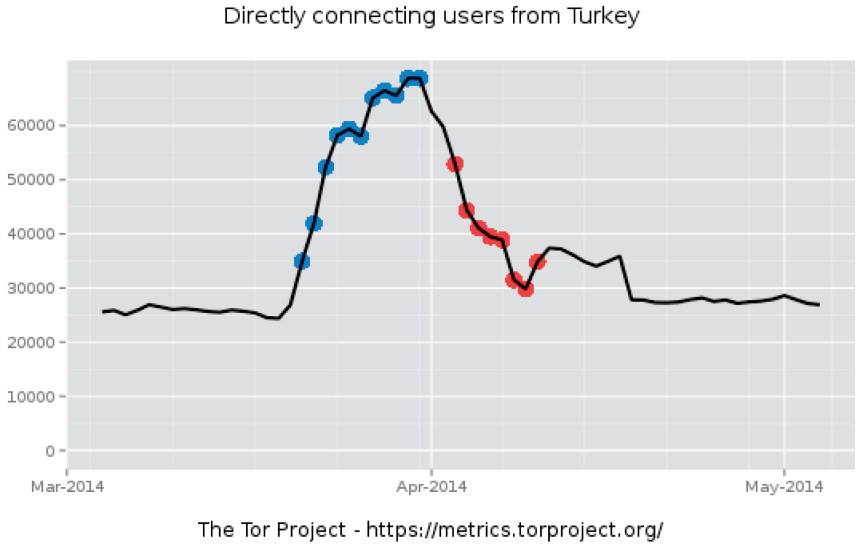
A participant, who describes themselves as 'a source with inside knowledge',[22] shared some metrics on Twitter traffic from Turkey. Although not possessing any 'hard numbers', the informant estimates that 'around 20% of the total number' of Turkish Twitter accounts connected from a non-Turkish Internet Provider (indirect evidence of people connecting via

TOR or foreign VPN providers). Moreover, 'around 50–80% of this traffic remained there two months after the ban was lifted, which was a little surprising'. This attitude to maintain some control over their Internet privacy, even after the events, is confirmed by all interviewees (mostly VPN users):

> I currently use an open DNS number and have access to blocked sites,[23] but I'm considering to buy a yearly plan on TunnelBear [VPN] **so that I can browse privately**.
>
> In case of any future blockage **especially on social networks**, yes I will definitely use VPN services again.
>
> Q: Are you going to use VPN again? A: **If there is further blockage**, yes.
> Q: Will you use TOR again? A: Still running and will do! Q: What's your experience? A: Experience? **I fell in love** with it! (Online interviews, emphases added)

> TBB is fool proof. It is easy to use. No need to install and configure software as TBB is ready to run. So many people began to switch to TOR or TBB. It was Twitter, forums and Bulletin Board Systems that made TOR famous. TBB was the key for its adoption. (Online interview)

I contend that the expertise and reflexivity which technology users acquire cannot simply vanish. Multitude's ability to learn, store and eventually perform, *unacknowledged*, the fruit of its immaterial labour is absolutely crucial (see Virno, 2003). From my first findings on the Turkish case study, I would additionally argue that many Internet practices transverse through lines of activism, use and production of digital data, so to encompass a broader, non-technology savvy multitude of users. These create, maintain and amplify the 'informational milieu' (Terranova, 2004) which



While VPN statistics are largely private, TOR Project publishes all network traffic on their website[24]: there is a sharp increase in TOR traffic after censorship blocks in Turkey (blue dots) and a progressive reduction, confirming the release of censorship after the elections (red dots).

TOR actually works. It is in fact easy to set up as a relay, in a way that users can share their bandwidth with the anonymous network. It is even easier if a user wants to just access the network without hosting any part of it, by installing a modified version of Firefox called TOR Browser Bundle, TBB.

supports more conventional hacking practices. For instance, users participate in a newsletter, ask for help or spread 'proper' hackers' workarounds through social networks or over material surfaces[25]:

> I worry about the population's huge percentage who does not know English. I kindly request a TOR browser pack in Turkish language for this. I hope **you guys** share the same responsibility as I feel . . . I can provide my service for translating every text in the browser to Turkish. (TOR-talk mailing list, 26 March 2014)

Here there is a demand, an offer for help and an initiation of a dialogue with 'you guys', presumably TOR developers and 'proper' hackers. Alleyne's distinction of three main strands of activities which characterise 'hackers' comes in useful here: open/clandestine practices, hacktivism and hardware hacking (2011). He suggests an 'integrated sociological understanding of hacking', which comprises these diverse set of practices:

> The hack is no longer the exclusive act of the hacker. When we make a web mash-up, a music or video remix . . . we are also part of a blurring of the lines between hackers and everyone else . . . We are all hackers now. (Alleyne, 2011: 25)

At times this collaboration becomes more manifest in spaces of the everyday. My main participant from the TOR-talk mailing list, who defines themselves as a 'help desk, system and network administrator', narrates this vivid account of his progressive involvement in the Turkish events:

> . . . The majority were Twitter users **with their Twitter nicknames** asking for help to access Twitter via TOR . . . Second round of TOR questions were how to make it fast . . . Some users came up with questions about cloaking of TOR. **It put me in a situation that I did not anticipate.** I thought it was the end, but it turned out to be not. People began asking for hidden services[26] . . . I got a particular email message from someone. S/he offered to pay for my service. That was all. I discarded it because I was overwhelmed with all TOR, DNS, VPN questions. Same person contacted me via email again. It was the same mail sent again. I again discarded it. Same mail got into my inbox a few days later. The email was from a non-profit organization. I was asked not to disclose their name and location. They were short on cash and wanted to set up a hidden service for their interest groups which was vital for them. **They offered appraisal and blessings nothing more.** I accepted it. (Online interview, my emphases)

This account again manifests the sense of ordinariness (e.g. not encrypted requests with their Twitter handle) and the escalation to more complex hacking practices which require learning and support.

Following the new hashtag #GoogleDNSisBlockedinTurkey, my narrative of a 'hacking multitude' became clearer by the hour. It was supported by an increasing frequency of reflexive comments regarding the weird game being staged live on the Internet.

> Every Turkish citizen has become some kind of Internet expert/amateur hacker after the ban. (tweet, Istanbul)

> [The] whole Turkey will be computer geeks:) (tweet, Istanbul)

These comments seem to foresee an indistinct mass of people, a multitude in fact, ready to take some control, at least temporarily, on a complex regime of communication. The content of communication, the message itself, takes a back stage:

> I checked my personal and company Twitter accounts' newfeeds. Although it was like a ghost town after a couple of days, we decided to continue to tweet from the company's official account. (Online interview)

Despite my objectives are other than unpacking links between technological networks and activism, I find it symptomatic that Twitter felt 'like a ghost town'. This observation supports the thesis that, after all, Twitter might not be central to urban protests. For my focus, though, it is more important that my participant and his colleagues 'decided to continue to tweet'. Here, form prevails over meanings, it evades codification. The necessity to be present beyond data choke-points, which undeniably pushed Twitter trends, unmasks the performative aspect of data itself. In the above vignette, there is a clear disconnection between how the network is imagined ('citizen journalism', trends, global audience) and how it is experienced ('a ghost town').

Towards a 'hacking multitude'? Two propositions

My preliminary findings around Internet censorship in Turkey show that an *extensive attachment* to the possibility of acting beyond restrictions started appearing. Not that this is always possible or that everyone wants to do it, of course. However, Turkish users' responses give the sense of a growing contention around the 'network of networks'. This is partly due to the Internet growing more complex and articulated, certainly beyond traditional national jurisdictions.[27] In my study, there is some evidence – the spike in TOR metrics, the leaked insight that part of Turkish users' traffic was from an ISP outside Turkey and the qualitative data collected from online interviews and from Twitter – that tactics of resistance to Internet censorship are learned and amplified in unpredictable ways. In this final section, I briefly explore two research trajectories which can further develop the initial formulation of a 'hacking multitude'. They foreground some implications that this generalization might have for the political, cultural or economic processes more directly associated with data.

1. There is a solid argument in cultural studies around the ubiquitous presence of software in everyday

aspects of our lives (Kitchin, 2011). This presents a whole set of issues around power (Lash, in Beer, 2009), surveillance (Lyon, 2014) and production of value. Differently from traditional media audiences (TV, radio and papers), social media consumers are in fact also producers of data. We routinely share, tag, like and comment, so contributing to Big Data metrics. These actions are almost automatic, they have become part of daily routines, they maintain the flow, both as data and as practices of 'evil media' (Fuller, 2012: 171). In other terms, most uses of the Internet now involve some kind of 'prosumption', a form of free labour in the production of data (Fuchs, 2014; Hardt and Negri, 2000; Lazzarato, 2002; Terranova, 2000). But, what happens when there is a disruption to everyday production/consumption of data, such as a censorship attempt? To what extent is a 'hacking multitude' able to disrupt, change, or maintain data flow? And how is the concept of 'flow' in itself useful when set against non-linear and unpredictable processes of techno-tweaking?

2. This opens to a second tenet. If digital labour implicates a social process of learning, a sort of 'geological stratum' of technological knowledge (Hardt and Negri, 2000: 29), hacking can be imagined as a sort of *collective* learning curve, a repository for actions and resistance whenever the situation presents itself. I attempted to follow some of the excitement brewing around the Twitter ban in Turkey:

> Whenever they ban something, we learn something new. (tweet, Istanbul)
> Everyone has to learn now about VPN, DNS, and how [the] Internet works. (tweet, Istanbul)

The relentless learning from practices of digital labour foregrounds the possibility that software and digital technologies can be used in more *competent* and *reflexive* ways. The Turkish example brings some evidence towards this kind of argument, but more research is needed, especially around perception of TOR or other data encryption systems from the perspective of everyday users. To the extent that circumvention of censorships and protection of own privacy might become a 'hacking game' for a multitude of users, production, circulation and consumption of digital data can become widely affected with regard to its volume, variety and velocity. Moreover, by generating and replicating content over a banned platform, users of social media create data with a higher intensity of affect, both locally and across the globe. The text and photographs analysed here convey *the experience* of 'hacking' from an everyday perspective: the sense of enthusiasm, frustration and radicalisation implied in the participation in a 'hacking game'. Some of the individuals who managed to avoid Twitter censorship in Turkey, eagerly circulated insights learned during their digital labour. They shared tips and enjoyed a newly acquired status of 'hackers', among friends, colleagues and social media followers.

> It feels like fighting against Agent Smiths in [the] Matrix movie. (tweet, Istanbul)

Concluding remarks

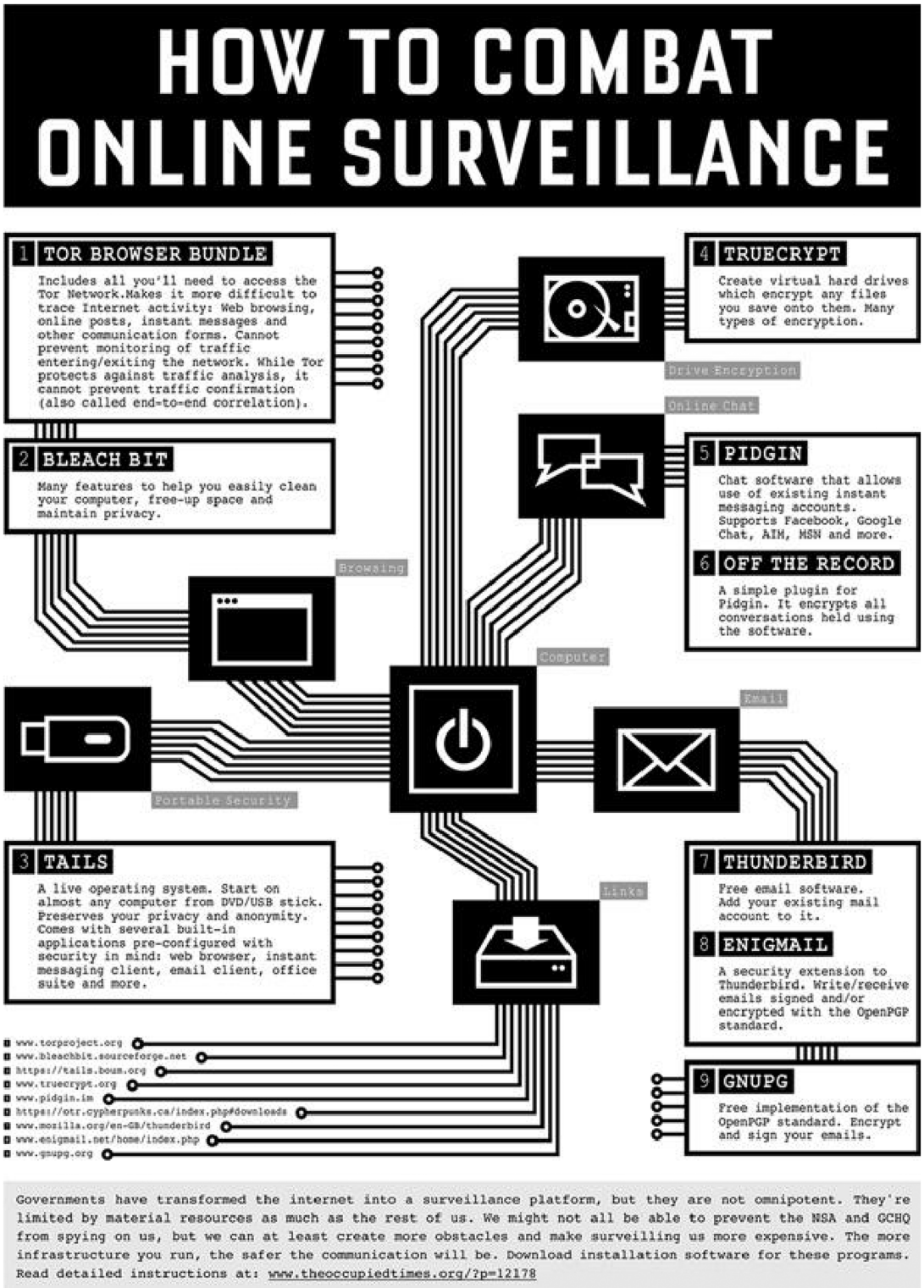
In trying to make sense of what happened in the Twittersphere when the Turkish government blocked access to the platform, I started looking at some Big Data metrics. These are in the form of infographics and statistics on Twitter traffic and trends. A solely quantitative analysis of Twitter data would give the impression that data flows seamlessly. But at a closer analysis, I would argue that the metaphor of 'flow' does not capture the immaterial forms of digital communication, *par excellence*: the sharing of bits in the form of a 140-character tweet. What became visible during the 'digital coup' were rather the materialities of social media systems – both the technological workings of the Internet with switches and routers, and the hacking practices of some of its users.

Censorship in Turkey gave space to a diffuse response that moved beyond the technological, what I try to capture with the concept of a 'hacking multitude'. The battle for presence on Twitter filtered down to inventive publics that probably had little to do with microblogging. Graffiti, banknotes, restaurant boards and so on were more than the circulation of a piece of information; they appear to be a legitimising stance towards Internet freedom. Although difficult to quantify in metrics of traffic, this social space cannot be neglected.

The composite scenario I engaged with suggests that there is a social, sensorial and affective dimension to the way in which we produce, defend ourselves from, or consume, the deluge of digital data. This dimension is emergent, plural and unstable, like data itself. Ruppert et al. argue that 'digital data is itself a materiality that is "alive," embodied and mobile', it actualises 'relations and connections that are otherwise beyond perception and thus inherent to the very imagining of social relations' (2013: 28). This means that attaining to data meaningfulness is a trans-disciplinary effort, beyond the statistical analysis of its occurrence. In the second part of the paper, I focused on individual responses by way of analysing some tweets, photographs and the content of online interviews. Digital ethnography and sociological discourse analysis are the methods I use to try to capture this media ecology made of pixels, tweets, censorship,

algorithms, bits and devices, but also of feelings, skills and frustrated attempts. This methodological approach attains to the particular and, therefore, to Small Data.

Working across – rather than simply mixing – quantitative and qualitative methods,[28] I started a reflection on an evolving scenario. The good thing about powerful visualisations, such as infographics, is the heuristic impression they give of a growing, and otherwise hardly accountable, exchange network (Ruppert et al., 2013: 36). However, it is the granularity of data itself, its



particular composition and diversity, which makes visible ordinary users' reactions. A 'multitude', in my focus. Within this varied ensemble of data, a privileged place belongs to photographs circulated by Turkish Twitter users. Photographs make explicit the interconnections between Big Data (in this case, tweets, trends and hashtags) and other communication systems (in this case, graffiti, banknotes, other social media and leaflets). These interconnections are performed in spaces of the everyday and possibly loaded with affect.[29] They are 'the social'. However, they are invisible in aggregate metrics of flow.

In the final part of the paper, I sketched the contours of what I emphatically called a 'hacking multitude'. This idea nests on a more general argument on Internet freedom. Deibert (2012: 17) calls the current stage of Internet relations 'Access Contested', pointing to a 'patchwork of competing interests and values' which will eventually define the Internet of the future. Similar to my argument, he talks of a 'multitude of actors'. Differently, he privileges institutional actors with a stake in cyberspace policies and practices on either side of the coin. These include giant corporations, civil society groups and 'public opinion'. It is in this novel reconfiguration of cyberspace that we need to set localised actions of ordinary people, such as forms of encryption or bandwidth sharing. These practices might look ingenuous. However, they form a sort of collective repository of a multitude that, creatively and opportunistically, reacts to censorship and surveillance of the Internet. They naively expose how this communication and data creation system is open to modification.

Declaration of conflicting interests

The author declares that there is no conflict of interest.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Notes

1. 'Twitter is a menace to society, to all societies. All kinds of immorality takes place there, families get separated; this is against the party's conservative agenda'; 'All our national, moral values have been put aside' (various sources).
2. 'Twitter and all – none of them are bigger than our nation' (Speech in Bursa, Turkey; Reuters http://tiny.cc/ssucnx).
3. Neither did I interview taxi drivers in Istanbul. I take this last point from satirist Karl Sharro: http://www.karlremarks.com/2013/03/its-ever-so-simple-tribal-map-of-middle.html
4. The concept of 'field' is obviously contested, and evermore so when related to virtual or digital ethnography.
5. http://www.theguardian.com/uk/2011/dec/07/twitter-riots-how-news-spread (LSE and the Guardian).
6. See campaign from Istanbul-based NGO, the Association of Alternative Informatics, who organised the recent Internet Ungovernance Forum (September 2014) in Istanbul, about the strengthening of Internet law 5651, central filtering, and the adoption of very controversial Deep Packet Inspection (DPI) software, like Phorm.
7. A 6000-member social media team of 'young, tech-savvy party members' are said to have been hired and trained to counter the Gezy Park movement on Twitter (*Wall Street Journal*, September 2013). See also Morozov (2011).
8. Wikipedia, various articles.
9. Hashtags are aggregating tools. They are increasingly popular in social media analysis in order to make sense of the vast array of messages exchanged on the popular microblogging platform.
10. Helsinki-based digital security company that produces Freedome. This is a mobile app which promises to completely anonymise its users by, among other things, setting your virtual location to a different country. The WSJ reported a similar percentage, citing Brandwatch, a firm that analyses social media analytics. 'The data, which took a sample set of geolocated tweets over a two-hour period, underscored how the ban appears to be backfiring'.
11. According to data provided to @Mashable by Sysomos, a social media analytics company.
12. We obviously don't know how many of these are real.
13. Demographer Conrad Hackett has a solid record of publishing statistics on Twitter in the form of colourful infographics.
14. I would like to thank online participants who circulated my research blurb through their social media connections, and those Turkish users who replied with enthusiasm. Since it was not possible to have explicit consent from every tweep involved, their responses have been carefully anonymised. This obviously includes their Twitter, Skype or email 'handle'. All respondents who spoke about TOR demanded an encrypted email exchange, anyway.
15. Here, I adapt Hine's '3E' framework of Internet culture: embedded-ness, embodiment and everydayness (2013).
16. Various online Latin dictionaries.
17. 'We stand with our users in Turkey who rely on Twitter as a vital communications platform. We hope to have full access returned soon' @Policy.
18. The 'Great Firewall of China' (Deibert, 2008).
19. This can be seen as a form of network surveillance that might infringe personal freedom, privacy, confidential business activities, relationships and state security (See Lyon, 2014).
20. My TOR connection does exactly that, with random exit points throughout the world.
21. For more information, visit TOR project blog: http://tiny.cc/3za2jx. The Russian Ministry of Internal Affairs has issued a $111,000 open call for Tor-cracking proposals: http://tiny.cc/cya2jx.

22. I did my best to check that my participants were who they said (cross-checking) and/or that they were referred by other participants (snow-balling).
23. More than 50k websites and twitter accounts are estimated to be banned in Turkey at the present (source: Internet Ungovernance Forum https://iuf.alternatifbilisim.org).
24. Source: http://tiny.cc/4s5jnx. Details about how this estimate is worked out: http://tiny.cc/h44jnx: 'We can't say how many distinct users there are... We really count clients, but it's more intuitive for most people to think of users, that's why we say users [there can be more users behind each client]'.
25. Similar recognition seems to start taking place in software culture. Reward Badges in Libreoffice project acknowledge 'an active contributor with zero experience in development, who helps in many other ways: translating users' guides, helping users on mailing lists and forums, writing wiki pages, etc.'
26. These are .onion domains not in the DNS system, they are only reachable via the network of TOR servers.
27. This argument can go either way of course: US NSA is now well known for having spied on emails and other traffic in many other countries.
28. See this discussion on Digital Sociology, http://tiny.cc/yoimnx.
29. The affect of whoever not only took and circulated the photograph, but also the affective experience of hacking, whether by coding or spraying a DNS number.

References

Alleyne B (2011) *'We are all hackers now': Critical sociological reflections on the hacking phenomenon*. Working Paper, pp.1–32.

Becker H (2002) Visual evidence: A seventh man, the specified generalization, and the work of the reader. *Visual Studies* (17): 3–11.

Beer D (2009) Power through the algorithm? Participatory web cultures and the technological unconscious. *New Media & Society* 11(6): 985–1002.

Couldry N (2012) *Media, Society, World: Social Theory and Digital Media Practice*. Cambridge: Polity.

Crary J and Kwinter S (eds) (1992) *Incorporations*. New York, NY: Zone.

Deibert R (ed) (2008) *Access Denied: The Practice and Policy of Global Internet Filtering. The Information Revolution and Global Politics*. Cambridge, Mass: MIT Press.

Deibert R (2009) The geopolitics of internet control: Censorship, sovereignty, and cyberspace. In: Chadwick A and Howard PN (eds) *Routledge Handbook of Internet Politics*. London: Routledge.

Deibert R (ed) (2012) *Access Contested: Security, Identity, and Resistance in Asian Cyberspace*. Cambridge, MA: MIT Press.

Fuchs C (2013) *Social Media: A Critical Introduction*. Thousand Oaks, CA: Sage Publication.

Fuchs C (2014) *Digital Labor and Karl Marx*. New York, NY: Routledge.

Fuller M (2005) *Media Ecologies: Materialist Energies in Art and Technoculture*. Cambridge, MA: MIT Press.

Fuller M (2012) *Evil Media*. Cambridge, MA: MIT Press.

Furman I (forthcoming) Peer production as alternative media: A study of Ekşisözlük's role in the 2013 Gezi protests. In: *Mapping the Alternative Media in Turkey*.

Georgiou M (2013) *Media and the City: Cosmopolitanism and Difference*. Cambridge: Polity.

Gerbaudo P (2012) *Tweets and the Streets: Social Media and Contemporary Activism*. London: Pluto.

Hardt M and Negri A (2000) *Empire*. Cambridge, MA: Harvard University Press.

Hine C (2000) *Virtual Ethnography*. London: Sage.

Hine C (2013) Christine Hine on virtual ethnography's E3 Internet. *Ethnography Matters*. Available at: http://tiny.cc/z13eux (accessed 20 February 2015).

Kitchin R (2011) *Code/Space: Software and Everyday Life*. Cambridge, MA: MIT Press.

Knowles C and Sweetman P (2004) *Picturing the Social Landscape: Visual Methods in the Sociological Imagination*. New York, NY: Routledge.

Lazzarato M (2002) From biopower to biopolitics. *PLI: Warwick Journal of Philosophy* 13(2): 100–111.

Leetaru K, Wang S, Cao G, et al. (2013). Mapping the global Twitter heartbeat: The geography of twitter. *First Monday* 18(5). Available at: http://journals.uic.edu/ojs/index.php/fm/article/view/4366 (accessed 14 October 2014).

Lyon D (2014) Surveillance, Snowden, and Big Data: Capacities, consequences, critique. *Big Data & Society* 1(2). Available at: http://bds.sagepub.com/lookup/doi/10.1177/2053951714541861 (accessed 13 July 2014).

Mackenzie A (2008) Wirelessness as experience of transition. *Fibreculture Journal* 13. Available at: http://journal.fibreculture.org/issue13/issue13_mackenzie_print.html (accessed 28 February 2015).

Morozov E (2012) *The Net Delusion: How Not to Liberate the World*. London: Penguin Books.

Mackenzie A (2011) *Wirelessness: Radical Empiricism in Network Cultures*. Cambridge, MA: MIT Press.

Murthy D (2013) *Twitter: Social Communication in the Twitter Age*. Cambridge: Polity.

Ruppert E (2011) Population objects: Interpassive subjects. *Sociology* 45(2): 218–233.

Ruppert E, Law J and Savage M (2013) Reassembling social science methods: The challenge of digital devices. *Theory, Culture & Society* 30(4): 22–46.

Steyerl H (2009) In defense of the poor image. *E-Flux*, no. 10. Available at: http://www.e-flux.com/journal/in-defense-of-the-poor-image/.

Terranova T (2000) Free labor: Producing culture for the digital economy. *Social Text* 18(2): 33–58.

Terranova T (2004) *Network Culture: Politics for the Information Age*. London: Pluto Press.

Underberg NM (2013) *Digital Ethnography: Anthropology, Narrative, and New Media*, 1st ed. Austin: University of Texas Press.

Virno P (2003) *A Grammar of the Multitude: For an Analysis of Contemporary Forms of Life*. Cambridge, MA: Semiotext (e).