Poletti and Michieli *City Territ Archit* (2018) 5:20
https://doi.org/10.1186/s40410-018-0096-2

City, Territory and Architecture

RESEARCH ARTICLE Open Access

Smart cities, social media platforms and security: online content regulation as a site of controversy and conflict

Chiara Poletti[1*] and Marco Michieli[2]

Abstract

Smart, technologically managed city-regions are one of the main characteristics of the contemporary world. Since the attack to the Charlie Hebdo offices, city-regions and social media digital technologies have increasingly been changing the definition of 'territory of security' and 'security governance'. What are the characteristics of the security architecture created by the interaction of smart city-regions and digital technologies? Drawing from Actor-Network theory and Science and Technology Studies, we provide an empirical account of the shape of this new territory, by presenting a study of the controversy concerning security and social media in UK, the role of cities in this changed security space, and how social sciences can help better understand and respond to the opportunities and threats of smart cities.

Keywords: City regions, Smart cities, Digital technology, Social media platforms, Security policies, Actor-Network theory

Introduction

Security policy has always been a national government prerogative. However, private transnational corporations and city-regions are an increasingly important site in the political and physical space of security policies. Firstly, privately owned technologies are both a source of insecurity (e.g. cyber attacks, online abuse, extremism, terrorism) as well as a tool of enforcement of security policies (e.g. filtering, censorship, and surveillance of users' data). Furthermore, global cities and citizens have become the real target and crucial node of contemporary security issues (Tebaldi 2016).

We define "architecture of security" the specific world-view and territories designed by the actors defining security threats and their modes of operation. It is increasingly transnational and hybrid, detached from the national territory and polity. It involves a large number of heterogeneous actors simultaneously occupying transnational, national, metropolitan, as well as private/public and human/non-human fields. What are the characteristics of this composite security structure? To answer the question, we investigate the public controversy related to social media (SM) platforms and security, initiated with the *Charlie Hebdo* attack in 2015. Applying Actor-Network theory and Science and Technology Studies lenses to the study of security we reconstruct how individuals, organisations and technology (i.e. social and technological actors) perform and enact the architecture of security by creating material and discursive associations. In particular, we utilise the methodological tools developed within controversy mapping to identify the actors involved in the redefinition of security in UK, with particular attention to the place occupied by technology and (smart) city-regions, and their position in the issue concerning Social Media (SM) platforms.

*Correspondence: polettic@cardiff.ac.uk
[1] School of Social Sciences, Cardiff University, Cardiff, UK
Full list of author information is available at the end of the article

Smart city regions and Social media platforms

The world is continuing to urbanise, and by 2030 sixty per cent of the world's population is projected to be urban (UNDESA 2016). City-regions[1] have become the preferred targets for attacks against collective security, driving city authorities to be increasingly involved in the management and enforcement of security policies (Tebaldi 2016). To face the challenges of these highly populated territories, city-regions are increasingly relying on new technologies. Smart cities are based on the idea of achieving sustainable development and a high quality of life thanks to the 'smart' use of human and social capital and technologies (Dameri 2013, Giffinger et al. 2007). Smart cities rely on data and the idea of algorithmic management of life: traffic data to develop intelligent transportation systems, medical data for health policies, feedback data for policies development and so on. From this point of view, smart cities and online platforms are of reciprocal interest. Online platforms are "digital infrastructures coordinating access to services, products, data, and content, primarily through algorithmic matching" (Casilli 2017, p. 2068). Online platforms appeal to the management of smart cities, as they are in control of the collection and gathering of data and metadata from users/citizens. At the same time smart cities represent an essential market for platform companies, which, like Uber or Airbnb, are increasingly involved in the management of cities (Gregory 2018). Platforms technology can help developing smart cities, but at the same time can creates new threats. In this paper we focus on the controversial aspects related to the use of a particular kind of online platforms, social media (SM) platforms, as a means to inspire, coordinate and diffuse episodes of violence perpetrated in city-regions.

According to platforms' scholar Tarleton Gillespie, SM platforms are online sites and services that host, organize, and circulate users' content, without having produced or commissioned it, and that are built on an infrastructure that processes users' communication data for customer service, advertising, and profit (Gillespie 2017). Because of their communication potential, SM platforms are generally seen as a tool to improve and perform smart governance at urban level. For instance, municipalities of smart cities have used Twitter and Facebook platforms to improve communication and speed services provisions (Kumar et al. 2016; Dameri and Ricciardi 2014).

However, the interaction between SM platforms and cities-regions is changing the definition of threats and security at the global level. In particular, the content hosted on these platforms has increasingly become a security concern. Abusive, racist, misogynist, and paedo-pornographic content hosted on platform has been a problem from the platforms' invention (WEF 2013; Webb et al. 2015). Moreover, since the attack to the *Charlie Hebdo* offices on 7th January 2015, SM have been identified as an (inter)national security problem. Not only the viral spread of content that followed the attack (e.g. the viral diffusion of hashtags #Jesuischarlie, #JesuisAhmed), fuelled unprecedented violent and polarised reactions around the globe, but also online platforms appeared as the place where terrorists were recruited and radicalised (European Commission 2016).

The effect of SM platforms on the security policies of city-regions and the controversy around the necessity of stronger content regulation have mobilised a variety of actors at different levels and in different fields, each proposing a specific interpretation of the issue and of the ensuing architecture of security.

At the EU level, 2 months from the attack (i.e. March 2015), a European Internet Referral Unit (EU IRU) was created within Europol, with the mandate of analysing and assessing content that might be rated as inappropriate or dubious. At the end of May 2016, the European Commission reached an agreement with representatives of the biggest IT companies (Facebook, Twitter, Google and Microsoft) on a code of conduct that includes a series of commitments to fight the spread of illegal hate speech online in Europe, including the removal of illegal hate speech in less than 24 h (EU Commission 2016).

On November 2015, the UK government introduced the Investigatory Powers Bill to define more clearly surveillance powers and reform oversight for the state. More recently, in the Digital Economy Act it included the development of a "Code of practice for providers of online social media platforms" dealing with online bullying and extremism. Other initiatives (such as the creation of an ombudsman and a levy on SM companies to support the policing of online offences) were presented in Autumn 2017 as part of the government Internet safety strategy.

In June 2017, the German government introduced a law establishing intermediary liability for SM failing to take down content considered illegal within 24 h. In January 2018, French president Emmanuel Macron announced "increased transparency requirements for internet platforms" in order to make public the identity of sponsors; and a new emergency procedure that will allow a judge to delete some content, close a user's account, or block access to a website, in case of fake news.

[1] Despite its increasingly widespread use, there is no commonly accepted definition of what a city-region is. According to Rodríguez-Pose (2008) a city-region is "a core city linked by functional ties to a hinterland" and those ties "include a combination of economic, housing market, travel-to-work, marketing, or retail catchment factors".

City authorities have also been active in the implementation of security policies concerning threats connected to the use of social media, often in coordination with regional and national authorities, and with the involvement of local private actors (Eurocities 2016). As the main focus of terrorist attacks, city governments have increased their spending in online security policies, creating ad hoc services for monitoring and policing content (e.g. London Online Hate Crime Hub).

As a response, SM companies have updated their users agreements, "Terms of Service" (ToS) and "Community Standards" (CS) and put into place systems of automated and human content moderation. From December 2015, Facebook and Twitter have updated their internal policies several times and expanded the content moderator teams that review reports on the networks, in an attempt to stop extremist, abusive and violent posts. In February 2016, Twitter shut down 125,000 accounts for threatening or promoting terrorist acts. Similarly, all big SM companies have adopted new technological tools (e.g. artificial intelligence) and human moderators to regulate content on their platforms (Sophos 2017). In June 2017, the major Silicon Valley companies, i.e. Google, Facebook, Twitter and Microsoft announced the formation of the Global Internet Forum to Counter Terrorism (GIFCT).

However, a real agreement on how to define and address the threats posed by SM use and security responses has not been reached. European institutions, as well as national and city governments have been demanding that SM companies put in place forms of content regulation, often associated with legislations aimed at increasing state powers on data monitoring and retention (Jourova 2016; Shields 2017). Such attempts to regulate content on SM clash with the extensive free speech rules that apply in the US, where most of these companies have developed. Moreover, the policy initiatives adopted by EU governments and private corporations in the area of blocking, filtering and removal of Internet content have started to raise concern for human rights (EDRI 2016), especially for freedom of expression and access to information as urged by the Council of Europe (CoE) Secretary General Thorbjørn Jagland (2016) and the UN Special Rapporteur on freedom of expression, Kaye (2016, 2017).

The public controversy that is taking place about the definition of threats and security responses deriving from the encounter of smart city-regions and SM technologies has important effects on the global architecture of security and consequently on human rights and the model of democracy we want to live in. Social theory can provide theories and methodologies that can help to investigate the process that is taking place.

Summary of existing literature

In the last 30 years, scholars on governance and security studies have progressively focused on two main aspects: the end of nation state centrality, and the emergence of the interacting intervention of multiple actors, both at the national and at the local level (Kooiman 1993; Le Galès 1995; Lorrain and Stoker 1997).

At the national level, globalisation and trans-border flows of people and money transversely cut political borders, challenging the traditional distinction of inside and outside, and the 'Westphalian/hobbesian' idea of security as state prerogative. The architecture of security built on national borders is 'deterritorialized or debordered' (Kristensen 2008). Nation states are one of many "spaces" that are constituted around security issues, where different actors compete for the definition of the threats and security system (Adamson 2016). This changed architecture includes a wide range of spaces, such as global city-regions, cyberspace, and contributes to create 'global polity'.

At the local level, cities face a re-scaling process in the security field, while they emerge even more as "geopolitically charged spaces" (Luke 2004). Additionally, technology has involved private actors in the management of security, distributing the responsibility from government to the private-sector, especially in cyber security (Collier and Lakoff 2008). Even if States have the ultimate say on the legitimate use of force, outsourcing and collaboration with commercial companies are widespread common practices (Abrahamsen and Leander 2015).

In social theory, Science and Technology Studies (STS) and the specific branch of Actor-Network theory (ANT) seem particularly well equipped to investigate governance in decentred social architectures (Latour 2005). The two approaches study science and knowledge production to question the ontology of society and the relations of diverse heterogeneous people, animals, machines, and things to one another (Roosth and Silbey 2008, p. 451). In particular, Actor-Network theory treats everything in the social and natural worlds as "a continuously generated effect of the webs of relations within which they are located" (Law 2008, p. 141) and focuses on the associations, assemblages, networks of actors that cross-cut human/non-human, public/private, local/global and formal/informal dichotomies (Schouten 2014). Not surprisingly, STS and ANT have been increasingly employed in governance of technology and Internet governance research (among the others, Musiani 2014; Mayer and Acuto 2015; Müller 2015; Hofmann et al. 2016; Epstein et al. 2016). However, few studies on security issues have adopted an approach derived from STS or ANT (Schouten 2014; Binder 2016). This approach aims at highlighting both the discursive and material elements of

security and threats e.g. (in)security. On the one hand, it shows how the distinction between security and insecurity is created through language and the debate on certain topics. It depends on the ability of an actor or actors to 'speak' a threat into existence. For instance, exploiting the socio-imaginary of terrorist attacks to development of counter-terrorism technologies (Binder 2016).

At the same time, this approach focuses on the material elements of society, emphasising the role of technology, objects and materials. In particular, the interest is on the way in which technical artefacts, devices and practices, combined with people, create socio-technical arrangements (Callon and Latour 1981; Barry 2001, 2013). Socio-technical arrangements are the result of successful processes of association of heterogeneous elements (i.e. the famous concept of "translation", Callon 1986a, b; Callon and Latour 1981). Once they are stabilised, they are "black boxed" or "taken for granted", and the different elements composing the arrangement disappear and the architecture of security emerges. Applying ANT lenses to the study of security means reconstructing how individuals, organisations and technology (i.e. human and material actors) perform or enact security by creating material and discursive associations.

ANT/STS applied to security studies investigate the processes through which the distinction between security and threats emerge as an outcome of these associations, refraining from making a priori assumptions about the ontology of (in)security or the actors involved in the process. The relational idea of power highlights how formal holders of power are not necessarily the ones that exert it: governors are always 'potential' in so far as they are dependent on all the other elements to actually govern (Edwards 2016). In this way, groups or networks of actors that cut across traditional social structures (i.e. nation states) can emerge, like software architecture, filters and algorithms for content recognition, Terms of Services and Community Standards, managerial strategies, public/private agreements (European code of conduct), European/national/city-region legislation, law enforcement bodies, users, terrorist groups and so on.

Methodology

As underlined above, an ANT-informed approach of the study of security architecture is interested in heterogeneous elements (i.e. actors), and the associations through which they create and perform socio-technical arrangements. The most employed methodological application of ANT is called controversy mapping, and it is based on the idea that in public controversies, it is possible to observe the associations linking the different social actors, otherwise indistinguishable from their socio-technical arrangements. Controversy mapping isolates the actors that have taken a position on a matter that concerns them, the so-called *group concerné*, and their different perspectives/programme of actions (Whatmore 2009).

In this project we aim to investigate the "machinery behind the stage" (Latour 2008): the material and discursive elements that are actively contributing in shaping the architecture of security. Drawing from Marres and Rogers (2005), in this study we delineate the controversy following hyperlinks among web pages dealing with the issue of SM platforms and security threats and confront the results with data from British newspapers.

Digital tools have been increasingly used to identify the relations connecting key actors active in a controversy, exploiting the 'social traceability' created by digital mediatisation (Marres and Rogers 2005; Venturini 2010, 2012). Even if mapping complex debate dynamics using digital data can be complicated, as each tool and source of data presents its own specificities which need to be considered (Baya-Laffite 2017; Ruppert et al. 2013), it is possible to address the bias by adopting an empirical approach i.e. considering the role of the specific medium and technology in the way that the issue is shaped (Marres 2015).

Traces of the actors animating the controversy can be found in the form of content published online, as well as metadata, relationships and interactions, links, shared vocabularies and keywords (Rogers et al. 2015, p. 44). With this method we have performed three different studies, each aimed at identifying a specific aspect of the controversy around SM platforms, security and city-regions.

Study 1) Analysis of actors, *group concerné*. In this part we asked what are the heterogeneous set of entities that assemble, associate around the matter of concern?

Study 2) Analysis of the associations that link the different actors. Focusing on the controversy online, in this part we asked in what ways the actors relate to each other?

Study 3) Analysis of the different issues composing the controversy. In this part we have asked what are the different topics that contribute to create the larger controversy?

We follow the traces of the controversy in two different 'public' spaces: the "Internet", and British newspapers, in the period from January 2015 to March 2018. The starting date was selected on the basis of the massive debate that started with the Charlie Hebdo attack in January 2015.

Google.co.uk was repurposed as tool for research to collect data published online (Rogers 2009). The search engine was selected as 90% of Internet searches in the UK happen through this medium (BBC 2013). However, as big as Google has become, using it as the only source to describe a controversy would leave aside many aspects.

As stated by Venturini "search engines are not the web; the web is not the Internet; the Internet is not the digital; the digital is not the world" (Venturini 2012, p. 803). To mitigate the risk of neglecting elements, we also performed the analysis of the issue in British newspapers from January 2015 to March 2018.

The study focuses on the UK context. The choice is motivated by the fact that the country has been very active both at the national and local level in the debate on new threats to national security. At the national level, the UK has developed a specific counter-extremism strategy, the so-called 'Contest'. Based on four main areas of work, the strategy aims to stop people becoming terrorists or supporting terrorism (Prevent); to stop terrorist attacks (Pursue); to strengthen protection against terrorist attacks (Protect); to mitigate an attack impact, where it cannot be stopped (Prepare). The strategy itself defines how the national government should cooperate with local governments. Of all the areas of work, "Prevent" has the widest implications for local governments, given that it implies a wide range of sectors addressed by the risks of radicalization. For example, the Greater London Authority has defined several practices, such as: the Counter Terrorism Awareness Week, a campaign led by counter-terrorism police and partners which focuses on partnership working with businesses, stakeholders and the general public; information activities on online reporting through the red Stop button, a service that enables anyone who finds online content that they believe to be terrorist or extremist material to report it online; an anti-terrorist hotline; and, a Countering Violent Extremism (CVE) program that involves an in-depth consultation with experts and local authorities to identify the operational improvements that can be implemented to counter hate crime and violent extremism. On the other hand, the intervention on the other fields is more reduced. We can cite as an example the 'Victim Support line' for people suffering trauma caused by terrorist attacks. This kind of practice can be ascribed to the "Prepare" target. The Greater London Authority has recently undergone a transformation, following the Lord Harris Review into London's Preparedness to Respond to a Major Terrorist Incident (2016). As a result, the London CONTEST Board was created to provide a strategic lead in addressing London's threats, risks, and vulnerabilities in relation to counter-terrorism. The new institution works in conjunction with the London Resilience Forum and, above all, the Mayor's Office for Policing And Crime (MOPAC).

Results

Dataset

To empirically examine the controversy, we built a dataset including 170 URLs collected from Google.co.uk (date of search March 2018) and 2862 articles from UK newspapers (date range January 2015–March 2018). The data collection was based on keywords relative to security and SM platforms. In the case of data from Google.co.uk the list of keywords was selected after a preliminary study of Google trend topics in UK. The list includes synonyms of "social media/networking site", "threats", "security", "content regulation", "hate speech": *"Social Networking, Social Sites, Social Network, Social Networks, Social Networking Websites, Social Networking Sites UK, Social Networking Site, Social Networking Sites, Social Networking Service, Social Networking, Social Network Sites, Social Media Sites, Social Media Sites, Social Media Content, Social Media, Online Social Networking, New Social Media, Networking Sites AND* (*hate speech OR threats OR security*). In the case of Newspapers the list of keywords was selected after a preliminary study of newspapers' articles keywords and indexes as presented in the Lexis Nexis' Newspaper repository. The list includes *"social networking" OR "online social networking" OR "social sites" OR "social network*" OR "social media*" OR "networking sites" AND* (*"content regulation" OR "threat" OR "hate speech"*).

Drawing on Rogers et al. (2015) methodology for issue mapping, in order to map the controversy as it is visible online, we included in the dataset the first 170 results as presented by Google.co.uk. These include web pages (69%) and links to documents (31%).

In the case of newspapers, the data collected show that the *Daily Mail* and *The Mirror* contribute for almost one-third of the data, followed by *The Telegraph*, *The Independent* and *The Times*. All of them included their online and Sunday editions (Table 1).

Study 1) Analysis of actors, group concerné

We identified the actors from the URLs using the following categories: Academia (e.g. Universities, Academic research groups, University student associations), EU/International institutions (e.g. UN, Unesco, EU), Government and government bodies (National and Local Government, politicians), Media Platforms/Websites (e.g. Online version of newspapers, or websites with clear information purpose), NGO/Advocacy groups (e.g. Non-profit entities, might be foundations, or charities as well), Private companies (e.g. Social Media Companies (e.g. Facebook, Twitter) but also law firms, private research centres such as think tanks, web designers, television channels, or platforms with clear commercial purpose (i.e. e-commerce platforms, Amazon, E-bay), enforcement agencies (e.g. Crown Prosecution service, Met Police).

In newspapers, we classified the actors mentioned by adopting a code that made distinctions between public,

Table 1 Data collected per newspaper (%)

	2015	2016	2017	2018	Total
MailOnline	14.33	16.16	17.05	17.30	64.84
mirror.co.uk	15.67	18.45	13.74	7.30	55.15
Express Online	9.50	16.77	10.93	9.30	46.50
telegraph.co.uk	10.00	7.47	9.44	9.50	36.41
The Times (London)	5.17	6.25	9.44	8.50	29.35
The Guardian (London)	9.17	5.79	5.63	7.40	27.99
The Independent (UK)	1.50	6.10	9.77	10.00	27.37
The Sun (England)	3.33	3.66	5.63	5.20	17.82
The Daily Telegraph	4.00	3.51	3.48	5.00	15.98
Daily Mail (London)	3.67	1.83	4.30	5.70	15.50
independent.co.uk	9.83	3.20	0.00	0.00	13.03
The Sunday Times (London)	3.17	2.59	2.98	3.00	11.74
Daily MIrror	2.83	2.59	1.49	2.20	9.11
i-The Independent Print Ltd	1.33	1.37	2.48	2.40	7.59
The Independent—Daily Ed.	0.00	1.22	2.15	2.50	5.87
The Express	1.33	0.46	0.50	0.90	3.19
Daily Star	0.83	0.76	0.00	1.00	2.60
The Observer (London)	0.83	0.46	0.17	0.90	2.36
The Sunday Telegraph	1.00	0.30	0.33	0.30	1.94
Sunday Express	0.50	0.46	0.00	0.70	1.66
Mail On Sunday (London)	0.17	0.46	0.33	0.40	1.36
The People	0.67	0.15	0.00	0.20	1.02
Daily Star Sunday	0.50	0.00	0.17	0.30	0.97
The Independent on Sunday	0.67	0.00	0.00	0.00	0.67

private and civil society, as well as national and local authorities.

We identified as public actors all the institutions, public administration and public agencies at the national and at the local level, including police and military forces (code 01). The private actors consisted of all the private companies, such as media platforms and website or companies operating in the field of security (code 02). Lastly, we added a civil society code to account for the NGOs, advocacy groups, think thanks and academics contributing to the public debate (code 03). We also operated a distinction between the national (1) and the local tier (0) to give a satisfactory record of actions launched at different level of the state administration: we distinguished between local police forces operations and actions undertaken by police forces at national level. When it was not possible to assign a category, we assigned a value "null" (code -99).

Based on this essential codebook, all the data were coded by the authors independently. Then we worked in pairs to review the coding process and how the codes were assigned. Any difference in coding was then saved for discussion. We solved the problem of intercoder reliability by comparing and debating cases of coding disagreement.

Table 2 Number of categorised documents per year

	2015	2016	2017	2018
Coded	181	147	134	125
Null	419	510	470	876
Total	600	657	604	1001

The data collected can be summarised as reported in Table 2.

Different group of actors in newspapers and online contribute to create this controversy: British national press gives large space to national public bodies, while, the online space allows a larger presence of local governments, academia, NGOs, and private companies.

Set of entities/actors in newspapers

Overall, and even considering the individual years, the controversy surrounding SM platforms and security as reported in the British press is shaped mostly by actors belonging to the public sector (Table 3).

In 2018, the difference in presence between public and private sector is minor, probably due to the fact that the time span covers only 3 months. Facebook, Youtube and Twitter are the actors more mentioned in the private sector.

Community and Security Trust, Big Brother Watch, Human Rights Watch, London Citizens Community Organisation Alliance and the National Society for the Prevention of Cruelty to Children (NSPCC) appear as the most frequent NGOs/Advocacy groups mentioned in the press. Within the public sector, national institutions, agencies and bodies of government (either MPs, Governments or special committees) have the majority (Table 4).

Local actors in public press are mostly local police forces, principally involved in anti-terrorism operations. City and regional authorities and institutions are present as a "target", or location for attacks (i.e. Westminster Bridge, London Bridge, Finsbury Park, Parsons Green, Manchester Arena), and rarely as original sources of a discussion on the type of threat and management. Only a few results show initiatives from city/region level, the most visible among them being the 'anti-cyber crime Hub' which is locally funded. It is interesting to notice that the city-level politician, Mayor of London Sadiq Khan has acquired visibility in 2018.

Set of entities/actors online

In comparison, as stated above, the controversy traced in Google.co.uk represents a more varied set of actors (Table 5). In particular, it favours Academia, NGOs and Advocacy groups as well as private companies and local governments over national government bodies.

Table 3 Number of documents per group of actors

	Express online	Express online	Express online	Express online
Public	150	100	96	62
Private	17	37	35	55
Civil society	14	10	3	8

Table 4 Number of documents per national and local level

	2015	2016	2017	2018*
National	159	110	129	113
Local	23	39	6	12

* Three months

Media Platforms and Websites represent the majority of actors creating the controversy online but differently from the traditional press they are mostly media outlet specialised in technology. The controversy online does not include URLs of posts or traces from users left within SM platforms, however it shows how SM companies are taking part in the definition of the issue, through the recovery of documents that relate to their internal policies on content regulation (i.e. Terms of Services).

Study 2) Analysis of the associations that link the different actors

In order to explore further the controversy, we have considered the forms of associations linking different actors. One of the most employed methods to study the associations within actors in a controversy, in the case of actors derived from URLs, is to use a web crawler to identify all the connections (i.e. hyperlinks) that one actor might have with the others and to visualise them in the shape of a network (Rogers et al. 2015).

Table 5 Documents per type of actor (%)

Categories of actors	Examples	% of the total (n = 170 URLs) (%)
Media platforms/ websites	The conversation, the Register, Wired… and online versions of newspapers	30.30
Academia	University of Oxford, University of Cardiff	27.88
NGO/advocacy	Open Rights Group, Hope not Hate, Tech Against Terrorism…	24.24
Private company	Facebook, Twitter…	6.06
Local government	London City Government…	3.64
National government	Publications from the Home Office, Parliament	3.03
Think tank	Demos, Paccs research	1.82
Enforcement and police	Crown Prosecution Service…	0.61
International Organisation	Unesco	0.61
EU Institution	European Council	0.61

We performed the analysis of the network of hyperlinks connecting the URLs collected from Google.co.uk. We found that, even if less represented than in newspapers, actors representing public bodies at the national level are very central in the controversy online (Fig. 1).

Media websites (which is the largest category) are clearly well connected to the national institutions (i.e. government, parliament). Local governments are present, but not as well connected with the other actors, especially media outlets.

The city government of London (Fig. 2) results connected to NGOs/Advocacy groups (i.e. State watch and the UK associations of local police treasurers, PACCTS), and Academia (i.e. Social Data Science Lab).

This could confirm that the controversy as defined in the public press neglects the initiatives taken at the local level.

The network map also attests the larger role played by NGOs and advocacy groups in the controversy online. These actors are much less visible in the public press. Figure 3 shows how State Watch (i.e. NGO that monitors the state, justice and home affairs, security and civil liberties in the European Union) for instance is particularly well connected in the network. It has links to other NGOs (e.g. Open Rights Group), news media (e.g. BBC, The times, telegraph), academia (e.g. University of Manchester, University of Oxford, London School of Economics (LSE), and the London Government.

Study 3) Analysis of the different issues composing the controversy

We tried then to understand how the issue of security is described in newspapers and online. We performed a quantitative analysis of the topics as presented by the actors in the documents. Concerning the newspapers, we extracted the most significant terms from the articles with the help of the website for text analysis developed by Cortext manager (Table 6).

The study of topics provides interesting insights in the discursive strategy (or programme of action) of the actors. "Terrorism", "national security", "fake news", "online abuse" and "personal data" are the most pressing issues that emerge within the articles (Table 6), while, "hate speech", "terrorism" and "security" are the most frequent issues mentioned in relation to SM platforms and threats on Google.co.uk (Table 7). Surprisingly, fake news appears as most pressing issue only on newspapers (probably due to the fact that online data collection is from the

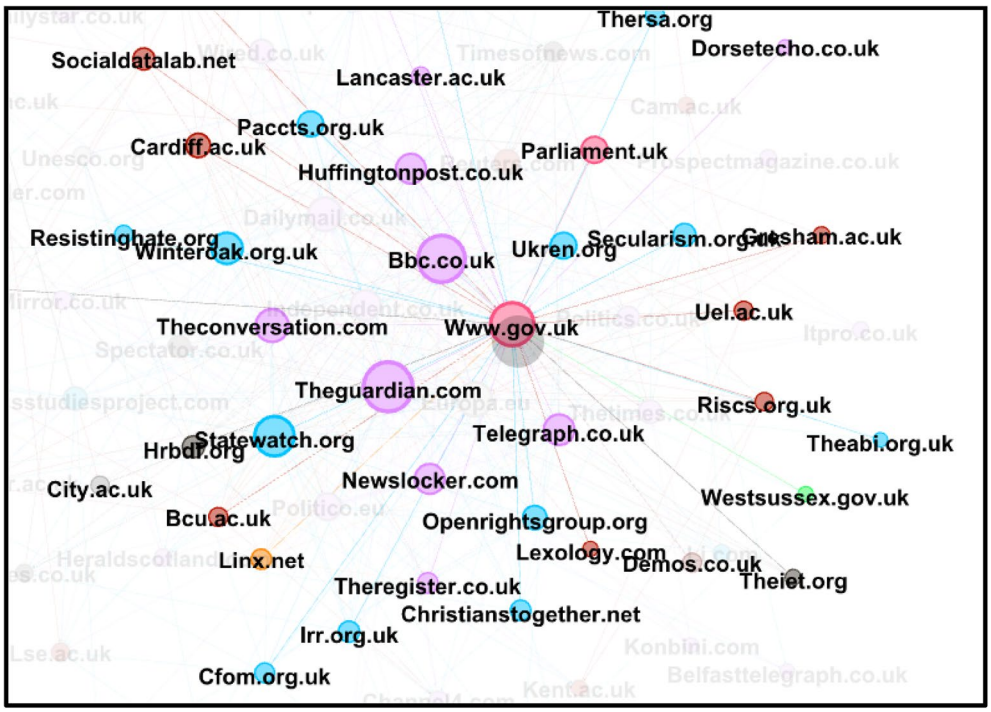

Fig. 1 National government, central actor (red node)

beginning of March 2018). Clearly terrorism and national security is the socio-imaginary which is mobilised the most with relation to threats and SM companies, not only in relation to the Charlie Hebdo attack, but also to the different terrorist episodes and violent attacks that took place in UK (i.e. Woolwich attack with the murder of Fusilier Lee Rigby in 2013, Salman Abedi and the bomb in Manchester in 2016, London Bridge attack in 2017). City-regions are mentioned as part of the topic of urban security in the controversy online, but more generally they emerge as scenario of attacks.

Technology plays a pivotal material and discursive role in the definition of threats and enforcement of security. Technology, artificial intelligence, automatic filtering and monitoring and in general technological regulation are among the most present issues mentioned on Google.co.uk (Table 8).

In newspapers, the articles show how technology has been playing different roles in the discussions about threats connected to SM platforms. For instance in 2015–2016, technology was a concern because of encryption, framed as a threat from national security agencies. From 2017, technology has been increasingly seen as an ally in the response to threats online, thanks to automatic regulation of content via artificial intelligence, until gradually becoming again problematic actor in 2018. To give an idea of the change in the role played by technology in the definition of the threats, here we report some extracts from the dataset:

- *The Daily Telegraph (London)*, 2015-01-03: "The firms, including telecoms and social media companies, are indirectly helping criminals evade detection by dramatically improving encryption on their services following the Edward Snowden leaks on GCHQ tactics".
- *The Times (London)*, 2015-11-24: "The 77th Brigade, which was formed in January, will be equipped to carry the fight to the enemy on social media by launching psychological operations on Facebook and Twitter, for example. The 1st Intelligence, Surveillance and Reconnaissance Brigade will conduct electronic warfare on the ground".
- *The Daily Telegraph (London)*, 2016-01-08: "The world's biggest technology companies have rounded on the Government's so-called snoopers' charter, claiming that the new laws threaten to weaken encryption, demand companies gather more data about customers, and could place their own staff at risk".
- *The Guardian*, 2016-05-11: "Apple's Tim Cook defends encryption. When will other tech CEOs do so? More high-profile titans need to use their plat-

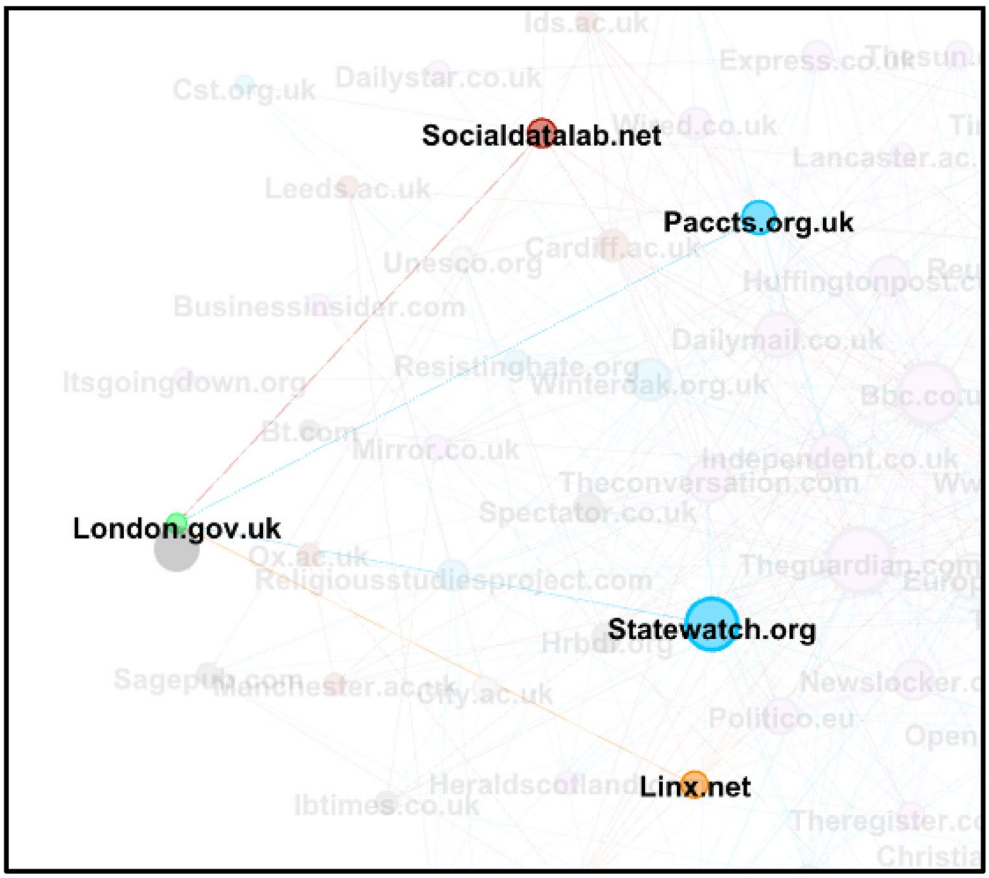

Fig. 2 London government (green node) direct connections

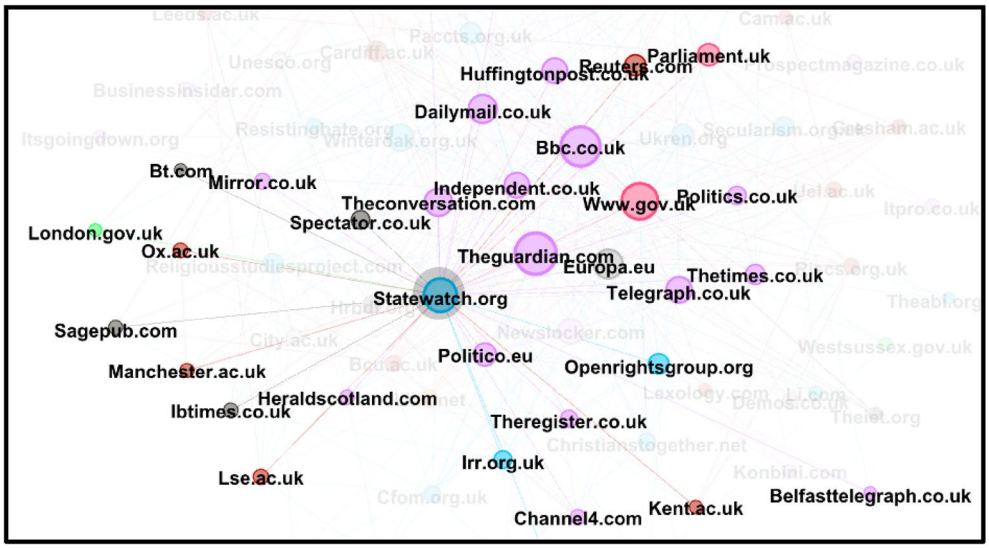

Fig. 3 NGOs are very central actors (blue nodes)

Table 6 C-value on topics presented by actors in newspapers

Stem	Main form	Forms	C-value
Attack terror	Terror attack	Terror attack|&|terror attacks	95.99200196
Group terror	Terror group	Terror group|&|terror groups	86.5501657
Twitter user	Twitter user	Twitter user|&|twitter users	72.38741131
Nation secur	National security	National security	37.76734503
Content extremist	Extremist content	Extremist content	36.19370566
Fake news	Fake news	Fake news	31.47278753
Propaganda video	Propaganda videos	Propaganda videos|&|propaganda video	28.32550877
Abus onlin	Online abuse	Online abuse	25.17823002
Data person	Personal data	Personal data	23.60459065

Table 7 C-value on topics presented by actors online (based on abstract of articles/web pages)

Stem	Main form	Forms	C-value
Attack terror	Terror attacks	Terror attacks|&|terror attack	11.01547563
Home offic	Home Office	Home office	11.01547563
Act secur	Security Act	Security act	11.01547563
Attack terrorist woolwich	Woolwich Terrorist Attack	Woolwich terrorist attack|&|woolwich terrorist attack	7.942847232
Nation secur	National security	National security	7.868196882
Attack terrorist	Terrorist attack	Terrorist attack|&|terrorist attacks|&|terrorist Attack	7.868196882
Cyber secur	Cyber security	Cyber security|&|cyber security	7.868196882
Secur threat	Security threat	Security threat	7.868196882
Peopl young	Young people	Young people	6.294557506
Compani tech	Tech companies	Tech companies	6.294557506
Abedi bomber salman	Bomber Salman Abedi	Bomber Salman Abedi	5.957135424
Bomber salman suicid	Suicide bomber Salman	Suicide bomber Salman	5.957135424
Committe mp	Committee of MPs	Committee of MPs	4.720918129
Code part	Part of the code	Part of the code	4.720918129
Bridg london	London Bridge	London bridge	4.720918129
Content extremist	Extremist content	Extremist content	4.720918129
Hate-speech illeg	Illegal hate-speech	Illegal hate-speech	4.720918129

forms to make crystal clear how important encryption is to users everywhere".

- *The Guardian*, 2016-09-21: "MI6 to recruit hundreds more staff in response to digital technology; Worldwide intelligence agencies increasingly rely upon internet and social media rather than running of agents".
- *Mirror.co.uk*, 2017-06-16: "Asked why Facebook was opening up now about policies that it had long declined to discuss, [*Monica*] Bickert *[Facebook Head of Global Policy Management*] said recent attacks were naturally starting conversations among people about what they could do to stand up to militancy. In addition, she said, "we're talking about this is because we are seeing this technology really start to become an important part of how we try to find this content".
- *The Times (London)*, 2017-07-10: "Twitter has made changes including using artificial intelligence to identify and shut terrorist accounts. Google, which owns YouTube, is also developing AI to block illegal content".
- *Mirror.co.uk*, 2017-06-16: "Facebook will use artificial intelligence to detect and remove terrorist content on the social network; The AI will analyse posts and messages to detect whether they contain terrorist content".
- *Telegraph.co.uk*, 2018-02-21: "Artificial intelligence risks being exploited by terrorists to mount driverless car crashes and cyber attacks because the technology is being rapidly developed without thought for its downsides, Oxford and Cambridge researchers have warned".

Table 8 Online controversy categorisation of topics (manual categorisation, one topic assigned to each URL)

Topic	Percentage of frequency
Terrorism	18.82
Hate speech	15.88
Tech Regulation	11.76
Security	10.59
Children	2.94
Extremism	2.94
Religion	2.94
Islamophobia	2.35
Minorities protection	2.35
Freedom of expression/protection of press	1.76
Migrants/refugees	1.76
Technology	1.76
Urban security	1.76
Ads	1.18
Cyber crime	1.18
Economy	1.18
Harmful content	1.18
ICT4D	1.18
Journalism	1.18
Legal field	1.18
Police	1.18
Politics	1.18

- *The Independent (United Kingdom)*, 2018-02-13: "Isis videos targeted by artificial intelligence that can detect propaganda before it's uploaded; Developers hope to combat threat of lone-wolf attacks by 'cutting propaganda off at the source".
- *Telegraph.co.uk*, 2018-02-21: "Seamless fake video, personalised spam and driverless chaos: how AI could create a playground for terrorists and scammers".
- *Telegraph.co.uk*, 2018-02-21: "Artificial intelligence: The saviour of mankind or the end of the world?".

Discussion

Media and technological effects on the controversy

The results show how the controversy takes specific features according to the media and technological environment where they are developed. The controversy on Google.co.uk involves a plurality of actors, while on newspapers it tends to give more space to 'traditional' political actors, specifically national government. Consequently, the variety of topics present at the online level is greater than the ones available in newspapers. Even though the study of the relationships/hyperlinks structuring the controversy online confirms the centrality of national political actors, the different composition of the *group concerné* confirms that media and technological environments play a fundamental role in the structuring of the public controversy. Specifically, the public controversy as shaped in newspapers is more 'traditional' and much less varied and detailed that the one presents online, even though more 'updated' (i.e. fake news).

Actors

The analysis of the public controversy concerning SM and security within the UK shows that national institutions maintain a primary role in the discursive definition of threats and security. National public actors are the most represented in the public controversy, as presented in British newspapers. In the controversy online, although national public actors are numerically less in the group of actors mobilised, they are the best connected and occupy a strategic role within the issue-network.

Despite this national primacy, it seems interesting to observe some peculiar trends with reference to private actors and local governments. In general, the data confirm that to some extent SM platforms' technology is eroding the state-centred architecture of security. Both in the issue created through newspapers and online, private companies (mostly SM platforms) are among the most visible actors shaping the controversy. We should not discard the idea that it is not the private actors pushing in state security field, but it is quite the contrary: the state is trying to restore its authority in a space dominated by "companies and consumers on the one hand and criminal actors on the other" (Cavelty 2015).

The involvement of private companies raises a number of issues, related to the concept of governance *by* and *of* platforms (Gillespie 2017). On the one hand, SM platforms have acquired responsibility in terms of content regulation: especially since States cannot police or regulate contents on SM companies without their collaboration (Gillespie 2017). However, delegating or imposing policing power on private companies (i.e. governance by platforms) comes with the risk of subordinating security to the for-profit agenda of capitalist companies. This creates issues in terms of democratic legitimacy and the possible effects on human rights, especially with regard to the quality of communication and the management of users' data by these companies (see Cambridge Analytica). On the other hand, too much State governance *of* platforms risks abuse and ultimately chilling effects on freedom of expression (i.e. NSA state surveillance) (United Nations and Kaye 2016).

The data highlight smart cities as a material element that influences the shape of the controversy. City-regions are mentioned as target of attacks, the biggest trigger

elements in the development of the controversy. Despite the engagement of some of them in facing the security threats, they do seem to have as stronger role in the discursive definition of the controversy, especially considering the controversy as it is presented in newspapers. Local governments' efforts to assign roles and create associations (e.g. local policies to monitor and police hate speech and radicalisation on SM platforms) are more visible in the controversy on Google than on the national press. The scarce presence of city-region governments in the public controversy defined in newspapers is even more notable if we consider that London city government is deeply committed to counter-terrorism policies. In recent years the city of London has indeed been under a constant threat from international terrorism and it has defined several practices to face the threat from the terrorist or extremist activity.

Similarly, civil society occupies a very small part in newspapers, but a central role in the construction of the issue online. Again, the data confirm the presence of two different sets of actors, according to the public space considered for the analysis. What is confirmed is that in general, civil society (e.g. NGOs and Advocacy groups) is making efforts to influence the way that larger actors are defining security and threats, often by pushing on freedom of expression, child protection, and minorities.

Technology plays a fundamental role as it is both an element for the enforcement of policies, and at the same time, it acts as 'mediator', i.e. an actor that can change and challenge the original programme of action of the other actors involved in associations (Callon 1986a). It has very important consequences for the discursive and material shape of the associations in the controversy. When actors such as states and private companies push responsibility onto technology, it has the result of reinforcing the discursive idea that management of security can be dealt with through technology. It is reinforcing the idea that a technological and algorithmic management of public life is more efficient (e.g. the idea of smartness) and can create better results. On the other hand, technology plays the part of mediator, creating new problems (e.g. creating new opportunities for terrorists or hyper censoring or visibility of certain contents). The very same solution, thus, challenges the original programmes and forces the other actors to redefine the associations/roles assigned (introducing, for instance, human moderators).

Conclusions

ANT methodology can provide useful empirical tools for the study of the architecture of security in the context of digital platforms. Understanding the data as a controversy, it is possible to see how discursive and material elements concur in the creation of the contemporary architecture of security. The study of controversies on different public spaces produced insights on the way in which media and technological environments are contributing to create and structure the public discussion about the architecture of security. At the same time, the specific theoretical and methodological approach makes visible how 'new' actors are contributing to this architecture by highlighting more central and marginal actors. With this, smart cities emerge as a material pivotal element, even if national institutions still maintain the primary role in the discursive definition of roles and responsibility in the field of (in)security. States push for their centrality by increasing their responsibility on the matter of policing content on their platforms. The most evident result however, is the empirical assessment of how private companies and especially their technology have become essential actors in the definition of threats and security measures. Technology in particular plays a fundamental role in the construction of material associations that influence the architecture of security. It is, thus, important that research continues to develop theoretical and methodological tools to investigate and critically expose the effects that such a definition of security, based on the relationship between private companies and public actors, can have on society.

Authors' contributions
This article is the result of joint research undertaken by the two authors. CP conceived of the study, carried out the collection of data and drafted the manuscript. MM participated in the design of the study, prepared the theoretical and hypothetical framework of the analysis, and edited the manuscript. Both authors read and approved the final manuscript.

Author details
[1] School of Social Sciences, Cardiff University, Cardiff, UK. [2] Università di Pavia, Pavia, Italy.

Competing interests
The authors declare that they have no competing interests.

Publisher's Note

Received: 1 March 2018 Accepted: 25 September 2018
Published online: 13 November 2018

References

Abrahamsen R, Leander A (eds) (2015) Routledge handbook of private security studies. Routledge, London

Adamson FB (2016) Spaces of global security: beyond methodological nationalism. J Glob Secur Stud 1(1):19–35

Barry A (2001) Political machines: governing a technological society. Athlone, London

Barry A (2013) The translation zone: between actor-network theory and international relations. Millenium J Int Stud 41(3):413–429

Baya-Laffite N (2017) Moving beyond the digitalised and natively digital divide? Mapping climate policy debates in multiple spaces. In: Paper presented at the 3rd international conference on public policy (ICPP3) June 28–30, 2017, Singapore

Binder C (2016) Science, technology and security: discovering intersections between sts and security studies. EASST Rev Volume 35(4). https://easst.net/article/science-technology-and-security-discovering-intersections-between-sts-andsecurity-studies/. Accessed 11 Nov 2018
British Broadcasting Company (2013) http://www.bbc.co.uk/news/technology-23318889. Accessed 10 Nov 2018
Callon M (1986a) Some elements of a sociology of translation: domestication of the scallops and the fishermen of St Brieuc Bay. In: Law J (ed) Power, action and belief: a new sociology of knowledge?. Routledge, London, p 196
Callon M (1986b) The sociology of an actor-network: The case of the electric vehicle. In: Callon M, Law J, Rip A (eds) Mapping the dynamics of science and technology. Palgrave Macmillan, London, p 19
Callon M, Latour B (1981) Unscrewing the big Leviathan. In: Knorr Cetina KD, Mulkay M (eds) Advances in social theory and methodology. Routledge, London, p 275
Casilli A (2017) Venture labor| how venture labor sheds light on the digital platform economy. Int J Commun 11:4
Cavelty MD (2015) Cyber-security and private actors. In: Leander A, Abrahamsen R (eds) Routledge handbook of private security studies (Routledge, 2015), pp. 89–99
Collier S, Lakoff A (2008) The vulnerability of vital systems: how "Critical Infrastructure" became a security problem. In: Dunn M, Kristensen K (eds) Securing the homeland: critical infrastructure, Risk and Securitization. Routledge, New York, p 40
Dameri RP (2013) Searching for smart city definition: a comprehensive proposal. Int J Comput Technol 11(5):2544–2551
Dameri RP, Ricciardi F (2014) Using social networks in smart city: organizational challenges, synergies and benefits. In: Smart city: organizational challenges, synergies and benefits. ECSM 2014 University of Brighton, Brighton, UK 10–11 July 2014, p 120
Edwards A (2016) Multi-centred governance and circuits of power in liberal modes of security. Glob Crime 17(3–4):240–263
Eurocities (2016). http://eurocities.eu/eurocities/documents/EUROCITIES-statement-on-the-contractualpublic-private-partnership-on-cybersecurity-WSPO-A7WHZR. Accessed Apr 2018
Epstein D, Katzenbach C, Musiani F (2016) Doing internet governance: practices, controversies, infrastructures, and institutions. Internet Policy Rev. https://doi.org/10.14763/2016.3.435
European Commission (2016) European Commission and IT Companies announce Code of Conduct on illegal online hate speech. Brussels: European Commission. http://europa.eu/rapid/press-release_IP-16-1937_en.htm. Accessed 10 Nov 2018
European Digital Rights (2016) https://edri.org/edri-access-now-withdraw-eu-commission-forum-discussions. Accessed 10 Nov 2018
Frantzi K, Ananiadou S, Mima H (2000) Automatic recognition of multi-word terms: the c-value/nc-value method. Int J Digit Libr 3(2):115–130
Giffinger R, Fertner C, Kramar H, Meijers E (2007) City-ranking of European medium-sized cities. Cent Reg Sci Vienna UT:1–1
Gillespie T (2017) Governance of and by platforms. In: Burgess J, Poell T, Marwick A (eds) Sage handbook of social media. Sage, London
Gregory K (2018) The future of work. paper presented at public services international congress. Geneva, Switzerland; 2018. http://congress.world-psi.org/karen-gregory-talks-about-the-negatives-and-positives-of-computer-platform-capitalism/. Accessed 10 Nov 2018
Hofmann J, Katzenbach C, Gollatz K (2016) Between coordination and regulation: finding the governance in Internet Governance. New Media Soc 19(9):1406–1423
Kooiman J (ed) (1993) Modern governance: new government-society interactions. Sage, Thousand Oaks
Kristensen KS (2008) The absolute protection of our citizens: critical infrastructure protection and the practice of security. In: Dunn M, Kristensen K (eds) Securing the homeland: critical infrastructure, Risk and Securitization. Routledge, New York, p 63
Kumar H, Singh MK, Hupta MP (2016) Smart governance for smart cities: a conceptual framework from social media practices. In: Dwivedi YK, Mäntymäki M, Ravishankar MN, Janssen, M, Clement M, Slade EL, Simintiras AC (eds), Proceedings of the social media: the good, the bad, and the ugly: 15th IFIP WG 6.11 conference on e-Business, e-Services, and e-Society, I3E 2016, Swansea, UK, September 13–15, 2016, (vol 9844). Berlin: Springer
Latour B (2005) Reassembling the social an introduction to actor-network theory. Oxford University Press, Oxford
Latour B (2008) What is the style of matters of concern? Two lectures in empirical philosophy. Koninklijke Van Gorcum, Assen
Law J (2008) Actor-network theory and material semiotics. In: Turner BS (ed) The new Blackwell companion to social theory, 3rd edn. Blackwell, Oxford, p 141
Le Galès P (1995) Du gouvernement des villes à la gouvernance urbaine. Revue française de science politique, 57-95.
Lorrain D, Stoker G (1997) The privatisation of urban services in Europe. Routledge, Abingdon
Luke T (2004) Everyday techniques as extraordinary threats: urban techno-structures and nonplaces in terrorist actions. In: Graham S (ed) Cities, War and Terrorism: Towards an Urban, Geopolitics. Blackwell, Oxford
Marres N (2015) Why map issues? On controversy analysis as a digital method. Sci Technol Human Values 40(5):655–668
Marres N, Rogers R (2005) Recipe for tracing the fate of issues and their publics on the Web. In: Latour B, Weibel P (eds) Making Things Public: Atmospheres of Democracy. MIT Press, Cambridge (Mass), pp 922–935. ISBN 978-0-262-12279-5
Mayer M, Acuto M (2015) The global governance of large technical systems. Millennium J Int Stud 43(2):660–683
Müller M (2015) Assemblages and Actor-networks: rethinking socio-material power, politics and space. Geogr Compass 9:27–41. https://doi.org/10.1111/gec3.12192
Musiani F (2014) Practice, plurality, performativity, and plumbing: internet governance research meets science and technology studies. Sci Technol Human Values 40(2):272–286
Rodríguez-Pose A (2008) The rise of the "city-region" concept and its development policy implications. Eur Plan Stud 16(8):1025–1046
Rogers R (2009) The end of the virtual: digital methods. (Oratiereeks / University of Amsterdam, Faculty of Humanities; No. 339). Amsterdam: Vossiuspers UvA.
Rogers R, Sánchez-Querubín N, Kil A (2015) Issue mapping for an ageing Europe. Amsterdam University Press, Amsterdam
Roosth S, Silbey S (2008) Science and technology studies: from controversies to posthumanist social theory. In: Turner BS (ed) The new blackwell companion to social theory, 3rd edn. Blackwell, Oxford, p 451
Ruppert E, Law J, Savage M (2013) Reassembling social science methods: the challenge of digital devices. Theory Cult Soc 30(4):22–46
Schouten P (2014) Security as controversy: reassembling security at Amsterdam Airport. Secur Dialog 45(1):23–42
Shields J (2017) Baroness Shields' speech at the National Security Agency Delivered to the fifth Annual Intelligence Community (IC) Women's Summit. https://www.gov.uk/government/speeches/baroness-shields-speech-at-the-national-security-agency. Accessed 10 Nov 2018
Sophos (2017) How social media companies are using AI to fight terrorist content. https://nakedsecurity.sophos.com/2017/06/20/how-social-media-companies-are-using-ai-to-fight-terrorist-content/. Accessed 10 Nov 2018
Tebaldi M (2016) Security, city and democracy. City Territory Architecture An Interdisciplinary Debate on Project Perspectives 20163(17):2018. https://doi.org/10.1186/s40410-016-0050-0
UNDESA (2016) The World's Cities in 2016. http://www.un.org/en/development/desa/population/publications/pdf/urbanization/the_worlds_cities_in_2016_data_booklet.pdf Accessed 10 Nov 2018
United Nations, Kaye D (2016) Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. Geneva, Human Rights Council. Available at:http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/Privatesectorinthedigitalage.aspx?platform=hootsuite. Accessed 11 Nov 2018
Venturini T (2010) Diving in magma: how to explore controversies with actor-network theory. Pub Underst Sci 19(3):258–273. https://doi.org/10.1177/0963662509102694

Venturini T (2012) Building on faults: how to represent controversies with digital methods. Pub Underst Sci 21(7):796–812. https://doi.org/10.1177/0963662510387558
Webb H, Jirotka M, Stahl BC, Housley W, Edwards A, Williams M, Burnap, P. (2015) Digital wildfires: a challenge to the governance of social media?. In: Proceedings of the ACM web science conference, p 64. ACM, New York
Whatmore S (2009) Mapping knowledge controversies: science, democracy and the redistribution of expertise. Progress Human Geogr 33(5):587–598
World Economic Forum (2013) Digital Wildfires in a hyperconnected world. Global Risks Report. http://reports.weforum.org/global-risks-2013/risk-case-1/digital-wildfires-in-a-hyperconnected-world/. Accessed 10 Nov 2018