IAMCR Preconference Surveillance and Security in the Age of Algorithmic Communication
Original CFP:
http://iamcr.org/leicester2016/algorithmic-surveillance

July 26 2016, Ken Edwards Building, Lecture Theatre Room 2, Main Campus, University of Leicester.

Abstracts (alphabetical order)
Keynotes/Plenaries abstracts TBA

Alves, Artur Concordia University **and Dias da Silva, Patricia** Université de Montréal
arturjmalves@gmail.com
pdiasdasilva@gmail.com

Transparency and veillance potential in online service providers' transparency reports

This paper explores the potential of transparency and corporate social responsibility practices as a sous-veillance tool. Specifically, it focuses on transparency reports (TR) of online service providers (OSPs) as a tool to be mobilized in an emancipatory form of engagement with technological politics. TR are published by online service providers (OSP) in order to disclose information on government requests of data and user information. Specifically, online service providers have rushed to publish TR in the wake of the Snowden revelations. The evolution of TR in the last five years shows that they provide information to users about government requests for data, but also create a performative alignment between OSP interest in self-regulation and growing user concerns pertaining to privacy and freedom of speech. In this paper we argue that TRs provide opportunities for multidirectional accountability in the relations between corporate, governmental, and civil society. By providing information about data-sharing practices, TRs provide users and civil society in general with tools for sous-veillance (Mann 2004). Best practices in TR, such as may be found in OSPs such as Google or Microsoft, address societal concerns pertaining to ethical practices and users' rights (privacy and surveillance, freedom of speech and censorship, among others), and therefore reinforce mutual transparency. In this sense, TRs contribute to reduce the opacity of algorithmic management of communication in the closed systems of contemporary online digital communication. As an instrument that lends a certain degree of transparency to the management of online algorithmic sociability, TRs can be seen as contributing to a redistribution of control among users, corporations and governments. The study was conducted by way of a comparative analysis of 10 TR, addressing the information and statements included in the reports and relevant OSP policy statements. Among the main sources are members of the Global Network Initiative (GNI), such as Microsoft, Google, Twitter, Facebook, LinkedIn. The GNI's transparency and accountability policy is used to ascertain to what extent these practices are in line with their stated intent, and how these positions articulate with both with the ongoing discussion on the future of online freedom, and with the institutional arrangements of

online communication. We argue that, on the one hand, the political and economic interests of OSPs demand a degree of transparency and resistance to governmental requests for user data, and therefore a proto-alliance has developed on the platform of privacy rights and encryption. The demands of corporate competition, on the other hand, have excluded a more radical, mutually transparent approach regarding internal practices and data-sharing with third parties. The latter view has not received much scholarly attention. This paper contributes to the current debates on the freedom of speech and online transparency by suggesting a role for TRs in a technological politics that harnesses the ongoing synthesis of online speech (a property or modality of freedom of expression in the era of online sociability) and platform politics (the arrangements of power and authority in online intermediaries).

Andresani, Gianluca University of Hull and **Stamile, Natalie** University of Catanzaro
gianlucaandresani@ymail.com
natalinastamile@yahoo.it

It's a bad world out there: Taking liberty (out)with emergency

Historical circumstances have inexorably led to changes and radical transformations of the social, cultural and political order. Recent events that could be referred to under the label of the 'War on Terror' show dangerous symptoms of an alarming decline of democratic and legal institutions whose justifications are based on the time honoured notions of the rule of law, separation of powers, democratic deliberation and accountability. In the current theoretical, philosophical and legal debate on cybersecurity, the issue of the (ab)use of emergency powers is becoming increasingly prominent. It seems that recent and not anymore so recent terrorist events and attacks have all had a crucial and negative impact on the (international) rule of law and democratic accountability. All this entails a transformation of the concept of law either into a synonym of force and/or as just a policy tool to be judged according to criteria of efficiency, reliability, etc, which is furthermore devoid of *normative* content and subordinate to executive discretion in times of emergency. In this paper, we will first assess the arguments justifying such a stance in the academic debates. This will entail an engagement on the one hand with scholars such as Richard Posner who argue that the trade-off between liberty and security is a *relative* matter that has to be judged according to historical circumstances and geographical contexts. On the other hand, we will critically review the theoretical and philosophical merits of that tradition (which has followers on both sides of the political spectrum) that refers to Carl Schmitt whose stance is much more radical since the emergency that justifies the violation of liberty rights is conceptualized as *existential* and that leads inexorably to political decisionism and to the justification of a *permanent* State of Exception. We will next analyse two cases of recent use of emergency powers, i.e. the NSA case in the US and that of the so called Snoopers' Charter in the UK. From the comparative analysis it will emerge that in the policy area of counter-terrorism and cybersecurity the practices of the governments of the two countries are in fact broadly similar. We will then assess the arguments used and compare them with those in the academic debate. Finally, we will conclude with an alternative *procedural* proposal which *subsumes* traditional paradigms of law and link them to deliberative democratic politics. In this final section, we argue that a conception of (global) justice concerned with both *individual rights* and *moral duties* that promote the *common good* is required. The main claim of the paper is that even times of war

and/or emergency do not warrant extra-legal action and lack of democratic accountability.

Barrenche, Carlos, Universidad Javeriana Colombia
barrenechec@javeriana.edu.co

Garbage in, gospel out: Malicious data practices and accountability in surveillance systems

This presentation will use the lenses of critical data studies (Bowker & Star, 1999; Dalton & Thatcher, 2014; Kitchin & Lauriant, 2014) to examine how loopholes in surveillance systems at the level of data generation and management can foster malicious data practices among collection agents. It addresses the case of a surveillance system deployed in a Latin American city that collects and analyses geocoded historical crime data in order to identify crime hotspots and perform geographic profiling of so-called urban quadrants. The system produces statistical information on places, dates, time of the day, crime modality, criminal profiling and potential victims so police officers can be efficiently allocated across the city following an anticipatory or preemptive logic. Considering this surveillance system's reliance of human input data, their creators claim, it relies heavily on applying adequate data collection methods. However, when police officers themselves are placed as data collection agents, with a direct interest in the generation of data that may be used to audit their own work, these systems become subject to abuse. Drawing on interviews with the designers of the aforementioned systems, I will characterize some malicious data practices such as deliberate miscoding, deliberate delaying of data flows, deterrence tactics to prevent citizens to produce certain crime data, and design-induced lack of interoperability between databases, in order to contest the claims of efficiency and neutrality commonly attached to data-powered surveillance systems. Data is always political and serves particular interests. So the need to situate the analysis of surveillance apparatuses in the contexts in which the data that feeds them is produced.

Balakrishnan, Sreepriya R Dpt of Collegiate Education, Kerala
sreebala.priya@gmail.com

Materiality of algorithms and the role of intermediaries: Problematizing free speech in the web

The word ‘material’ had been long extended to the meaning and content of the object in Western phenomenology with Hegel’s understanding of the material and there was a significantly ‘material turn’ in the study of art and media with the tremendous changes in the modes of production that led to a de-auratization of art objects (Benjamin). Following this theoretical tradition of deauratizing, are those archaeologies of the present that considers the material and technical conditions that permit the discourse storage and distribution as elemental to the networks. (Kittler). The deeming of electronic media, internet and the web as ‘immaterial’ mediums and the understanding of what constituted the ‘cyberspace’ as a ‘virtual world’ looks very ironic in this context. In fact objects that are loaded with ‘virtuality’ are those that need to be scrutinized more for their seeming innocence. In the initial inquiries into the exposition of the virtuality of networks, hardware and devices were looked upon as ‘evocative’ or those that provoke

our thoughts.(Turkle). The larger research to stop viewing a network as composed of anonymous objects, to demystify its aura are now taken up in the inquiries about the physical making of software as objects (Fuller), the recursive algorithms that define the mechanical processes of digital computers (Parikka), and the integration of the concepts of database and algorithms in the ontology of computation (Manovich). This shift that primarily imply a shift from the ICT model to that of the Computation model has now opened up a plethora of questions regarding the materiality of programmable objects, especially when they are used as agents of surveillance and regulatory control. Materilality of virtual objects is not just about their physical constitution, but an "emergent property created through dynamic interactions between physical characteristics and signifying strategies." (Hayles) This paper attempts to look at the materiality of algorithms, the procedural logic that undergirds all computation that, no doubt has deep political potent (Gillespie), and thereby demystify some of the syntax structures that involves the constitution of algorithmic patterns in identity formations in web platforms that are run by the intermediaries. By taking what is referred to as 'new algorithmic identity' (Cheney-Lippold), the paper traces the evolving cultural patterns of the algorithms that define identity recognition by the intermediaries in three stages. The first stage is how user interactions were made to co-align with the framing of algorithmic identities in the pre-web 2.0 period in MUDs and dungeons. The second is when the ideology of Web 2.0 began to shroud identity formations and profile regulations in web, when the intermediary roles were getting forged technically. The third stage is when disputes between individuals and corporate intermediaries began to be taken out into the offline realms in legal contexts around the world where the questions about algorithms remain largely absent and beyond reach. Thus we may argue that the vulnerability of textual speech-acts in the social media are intricately layered with the cultural complexity and technical invisibility that algorithms generate and the use of the algorithms by the intermediaries. The vulnerability gets extended materially, culturally and legally when individuals clash with the media platforms over their rights for free expression in internet. Through the case study of a 'nymwar' in the Indian Facebook circle that was taken up by a few women who demanded that Facebook reconsidered its algorithmic and cultural standards, following a profile ban of a woman who openly defied the majoritarian nationalist norms, that led to a campaign called #for a better Fb, the paper traces the processes through which identity formations in web and legitimacy of speech acts gets entwined with the materiality of algorithms. By closely studying how the legality of speech acts are getting established through precedence in a series of legal jurisprudence into the role of the intermediaries, the paper leads to the fact that the relation between content and the intermediary is getting more and more solidified through the use and abuse of algorithms. This intermediary liability over content in turn implicates that private corporate censorship would not only be the framework for future directions in what is termed as 'free speech', but also that intermediaries would be inclined to create more and more sophisticated filtering algorithms that would help them to sieve every data and interpret every profile as single 'algorithmic identity', thereby challenging the early theories about the plurality of self in the web.

Brayshaw, Mike, Gordon, Neil University of Hull **and Karatzogianni, Athina** University of Leicester

An empirical investigation into perceptions of privacy, surveillance, and security: Are undergraduates actually bothered?

m.brayshaw@hull.ac.uk
n.a.gordon@hull.ac.uk
ak547@le.ac.uk

Do Undergraduate Students realise or care about the information they reveal about themselves or what Artificial Intelligence techniques can deduce from their online footprint? In the age of Social Computing there is a rush to establish a presence on Social Media. This started with simple web pages hosted by your ISP, your University, or early social media. This has developed into a world of Facebook, Instagram, Twitter and LinkedIn. Communication by email is an established - 30 year old -social norm; moreover, it was the start of an explosition of Computer Mediated Communciation that today extends to technologies such as SKYPE and FaceTime. However, this online activity all leaves a lasting record. Online activity, be it in terms of a Profile, TimeLine, New Feed, Likes, or Following, give away a lot of personal data. This is before we start to look at conversations and other computer mediated interactions. The old addage of "what's done in Vegas stays in Vegas" is no longer the case. On line activity leaves a record. These records can then be mined for information revealing previously hidden or unnoticed activity patterns. An unrelenting algorithmic assault on our online activity. To this context, we have to add the massive breakthroughs that have been announced in the AI field of Deep Learning and note the leading role that Facebook and Google are taking in this area (e.g. Tian and Zhu, 2016). Within this context, we wanted to find out if all this concerned students in their use of computers. To this end we undertook an empirical study with an online questionairre of Computer Science Students at the University of Hull, and Media and Communication Students at the University of Leicester, UK. The anonymous survey looked at Privacy and Security in Social Media and Online Sites. The survey consisted of 31 questions, an example of which is shown below:

When using social media (for example, Facebook, Twitter, WhatsApp), do you worry

- ☐ about who is going to read your message
- ☐ how long your post/message is going to be visible for
- ☐ who is going to record what you have said
- ☐ who might subsequently try to use this information

Tick box for yes.

The survey ran in December, 2015 and again in February/May 2016. This paper presents findings of our work. In particular, we will report on the following:

- Do students know where their data is going?
- Do students care about where their data is going?
- In the age of Algorithmic Communication does this issue concern students?
- Do they worry about their information being mined?

Reference:

Tian, Y, and Zhu, Y. Better Computer Go Player with Neural Network and Long-Term Predication, submitted to International Conference on Learning Representations, 2016.

Brevini, Benedetta University of Sydney
benedetta.brevini@sydney.edu.au

Between Big(Meta) data and journalism: Tracing the emergence of a new culture of discourse

In the launch edition of the new journal Big Data and Society, Couldry and Powell (2014) developed the argument that a question of agency is paramount to our understanding of big data. This call has opened up a new research agenda for investigating not only dominant forms of data power (Lash, 2007) but also alternative forms of datafication emerging from civil society groups, community organisations, activists and journalists. Thus this study takes up the challenge to further develop "social analytics" by focusing on practices of datafication and resistance by journalists in Australia. Australia is a significant case study to examine because in October 2015 its federal government has passed very controversial metadata laws that require telecommunications companies to retain metadata of their customers for a period of two years. The new acts pose incredible threats for the profession of journalists as they enable government's agencies to easily identify and pursue journalists' sources. Bulk data collections of this type of information deter future whistleblowers from approaching journalists, thus making it quite challenging to perform their democratic role. How do journalists in Australia respond to the new frameworks? What forms of datafication are Australian reporters developing? What new partnerships are emerging between journalists and activists? This paper attempts to shed light on these challenges and questions whether we are witnessing the emergence of a new digital culture of disclosure.

David Chandler University of Westminster
d.chandler@wmin.ac.uk

Securing the Anthropocene: Community hackers against the digital, A case study of Jakarta

This paper analyses security discourses that are beginning to self-consciously take on board the shift towards the Anthropocene. Firstly, it sets out the developing episteme of the Anthropocene, suggesting that this new epoch highlights the limits of instrumentalist cause-and-effect approaches to security, and suggests that knowledge is increasingly generated through new forms of mediation and correlation, capable of grasping or seeing non-causal relationships and interconnections. Key to this approach is the deployment of analogical thinking rather than digital forms of reductionism. It then goes on to draw out these approaches in the practices and imaginaries of securing the Anthropocene, using as a case study the field of digital humanitarianism and disaster risk reduction, with the focus on social-technical assemblages able to enhance the power of geo-social networked forms of collective intelligence, being developed and applied in 'the City of the Anthropocene': Jakarta, Indonesia. The paper concludes that policy interventions today cannot readily be grasped in modernist frameworks of 'problem solving' but should be seen more in terms of evolving and adaptive 'life hacks'.

Connelly, James University of Hull
j.connelly@hull.ac.uk

Speech acts, context and tempered agency in a digital world

The point of the argument is not to deny the distinction between public and private, nor to deny that law has to presuppose such a distinction. Rather the point is to problematise the distinction in two related ways. The first is to show that it is a politically negotiated distinction, not an inherent distinction antecedent to, and superior to, political negotiations. The second is to show that there are (and always were) many, various, fluid and overlapping distinctions between the public and the private; with the rise of digital technology there is an urgent need to extend our understanding of the complex nature of the relationship between the public and the private. Hence the paper begins with a discussion of the contested nature of the distinction between the public and private in which it is argued that privacy as a politically negotiated space rather than as an a priori good antecedent to politics. It follows from this that no hard and fast distinction between public and private is possible. Secondly, it addresses issues of individual responsibility, self censorship, and the nature of the speech act. In particular it addresses the changing nature of the speech act in cybersecurity and cyber contexts; the many different layered and overlapping contexts of utterance and action; the need to understand the context in which one is acting; the relationship between this and individual responsibility. By insisting on the need for tempered agency there is no implication that free speech should be curtailed. The argument addresses the self chosen appropriateness of an agent's speech. Some might argue that this is an argument in favour of so-called 'political correctness.' Political correctness is a vague and unhelpful term and, in this context, a red herring. People have always tempered their actions and speech. The issue facing us is the challenge of dealing with this appropriately in the digital age and to inquire into what difference the digital environment makes to how each one of us can or should or temper our speech and actions.

Dencik, Lina and Hintz, Arne Cardiff University
DencikL@cardiff.ac.uk
HintzA@cardiff.ac.uk

Datafied 'threats': Uses of social media for policing domestic extremism and disorder in the UK

This paper examines the uses of social media for policing domestic extremism and disorder in the UK. The collection and analysis of social media data for the purposes of policing forms part of a broader shift from 'reactive' to 'proactive' forms of governance in which state bodies engage in big data analysis to predict, preempt and respond in real time to a range of social problems. Although this promises for more efficient and objective forms of decision-making, an emerging body of work warns that uses of big data for governance may also contribute to forms of suppression, inequality, and discrimination. What is more, whilst the collection of data may provide opportunities to identify problems, risks and potential 'threats', the challenges of oversight, accountability and transparency involved in the collection and use of people's

information remain key concerns. This paper engages in these debates by looking specifically at how social media data informs decision-making with regards to the policing of domestic extremism and disorder, particularly in terms of protests, in the UK. Based on interviews with senior members of the British police force as well as big data analysis emulating practices of predictive policing of protests, this paper explores the nature and uses of algorithmically-produced intelligence emerging from social media big data. In particular, we contextualize this so-called 'Open Source Intelligence' (OSINT) within the history and regulatory framework of British policing practices and outline the types of tools and software that help inform pre-emptive and real-time strategies for policing protests in the UK. This is a relatively new development within British policing that depends to a large extent on marketing-driven software development. Such programmes identify phenomena such as 'threat-words' (e.g. 'flares'), risk assessment and resourcing (who and how many people will attend), and influencers and organisers (not always clearly distinguished). To a lesser extent, they are also used for sentiment analysis (mood of a crowd) and geo-location analysis (particular areas of gatherings). We argue that this context introduces a number of key issues regarding the changing nature of police practices that have significant implications for our understanding of the nature of the public, the meaning of crime and the role of policing. Also recognized amongst police themselves, we are confronted here with not only questions of privacy in the context of social media, but also broader concerns with accountability and transparency in the 'black-box society' (Pasquale 2015) of algorithmically-produced police intelligence that shifts definitions and management of potential social 'threats'.

Reference:
Pasquale, F. (2015) The Black Box Society. Cambridge, MA and London: Harvard University Press.

Gak, Martin Kosmopolitica - The Good Life Lab
martingak@gmail.com

The very hairs of your head: Hypernomianism and the digital reconstruction of theological models

Generally speaking, there are two theological accounts of the way in which the monotheistic god's omniscience guides human action. One goes more or less like this: because god knows all actions, none can be hidden. Therefore all punishment is both just and inexorable. The second is some form or other of theological determinism: god's knowledge of future events amounts to a causal constraint on freedom. This curious problem mobilized the intellectual attention of the early Augustine. In De Liber Arbitrium, Augustine tries to account for the way in which his god's omniscience can be compatible with free will. The problem for Augustine is of deep theological consequences. If god determines all actions, then man is not responsible for the plainly evident evil that he commits and this means that his god is not quite as good as presumed. The problem is not merely an arcane theological matter. The emergence of technological mechanism capable of registering the most minute facts of matters amounts to a form of disembodied omniscience. But such omniscience is digitally available to political and juridical wills. Not only does this knowledge is evidentiary

content for prosecutorial processes--juridical and political and moral--but it is capable of issuing in the articulation of newer norms.

Geesin, Beverly, York St John University
b.geesin@yorksj.ac.uk

Raising the surveillant subject: children with toys that are intelligent and interactive

Advances in artificial intelligence technology made popular by systems such as Apple's SIRI concurrent with an expanding market of products using technology such as wi-fi and RFID marketed under the umbrella term of internet of things are increasingly exploited in the consumer electronics market. Often, the promoted pleasures of connectivity and interactivity obfuscate issues of privacy and dataveillance. A subset of this growing market is a number of products marketed to children as interactive toys. Toys such as Hello Barbie, My Friend Cayla, Cognitoys' Dino and Jibo promise a varying level of intelligent, interactive companions. However, the functioning of these devices and the quality of the social interactions are largely dependent upon sending the interactional data back to the company in order to improve the artificial intelligence algorithms. How this data is stored and used has serious privacy implications. Further, there are also broader implications as children interact with these devices in regards to socialisation, educational development and communicative practices. At a time when such products are either just entering or about to enter the market there is a need to examine the many ways in which children's engagement with these toys is potentially problematic. Reflecting on the frequent adaptation of military technologies for toys Thrift (2006) argues that they are the gateway to the interactive world. The banality of toys can normalise and domesticate surveillance technologies. Such toys can render as mundane ideas or technologies which would otherwise be experienced as incoherent (Mosco, 2005). Further, the valorisation in sharing, interaction and visibility, upon which the functioning of these toys is dependent, normalises the consumption of surveillance. This paper examines these toys and the accompanying marketing rhetoric and considers them in terms of how they interpellate children as surveillance subjects through a socialisation which normalises monitoring as sharing and transactional and/or programmed conversations as meaningful interactions and relationships. Children need to be empowered and educated to use technology, understanding the implications for privacy, interaction and identity. The concern is that toys such as explored in this paper, instead, socialise children as prosumers and surveillant subjects normalised and complicit in their own monitoring by governmental and commercial organisations.
References:
Mosco, V. (2005) The Digital Sublime: Myth, Power and Cyberspace. Cambridge, MA: MIT Press.
Ritzer, G. and Jurgenson, N. (2010) 'Production, Consumption, Prosumption: The nature of capitalism in the age of the digital prosumer'. Journal of Consumer Culture, 10(1): 13-36.
Thrift, N. (2005) Knowing Capitalism. London: Sage.

Donyina, Adwoa Chapman University and **Heckel, Reiko** University of Leicester
donyina@chapman.edu

reiko@mcs.le.ack

A graph transformation model for peer-to-peer content policing

Extreme or illegal content in online social networks poses risks to individuals and society. Policing such content is often used as an argument for centralised surveillance. However, such a centralised approach to policing suffers from two drawbacks. First, the amount of data to be collected if content is to be policed comprehensively is prohibitive. Second, if centralised content policing is effective, it risks sacrificing privacy. An alternative, distributed policing model is inspired by Peer-to-Peer (P2P) networks designed to perform their function without centralised management. In such a model, individuals can strongly dislike (blame) inappropriate content they encounter and beyond a certain threshold aggregated blame from a number of individuals leads to content being banned or blamed to a central authority for evaluation. Such a protocol is potentially scalable and less intrusive, but it carries its own risks. 1. It is potentially sensitive to abuse of blame to suppress opposing views, harming freedom of expression. 2. It may not be effective enough in filtering out genuinely extreme content reliably. The sensitivity to abuse and reliability of a P2P policing protocol depends on a number of factors, including the amount of blame available in the network, the thresholds for banning or blaming content and the behaviour of the majority of individuals in the network. We are interested in exploring under which circumstances and parameters a protocol like this can deliver satisfactory results, to understand its potentials and risks. We approach this question by modelling the network's operation by graph transformation rules describing the creation and distribution of content in the network and the adaptation connections based on individuals' shared opinions. Adding rules for blaming and banning content and / or users with varying rates or probabilities we can explore how different behaviours and protocol settings influence the overall outcomes. The model includes a type graph describing the different types of nodes and relationships of interest and basic operations by means of rules to manipulate the graph. Such models can be executed directly by a simulation tool as well as translated into mathematical models of differential equations to allow validation as well as quantitative analysis.

Garnett, Philip University of York
philip.garnett@york.ac.uk

Chasing Rainbows: A search for transparency in the use and design of security and financial algorithms.

Potentially arbitrary programming decisions have numerous material effects on the world. The technique applied, the position of thresholds, variable choice, and the training data used. Together these and other factors determine if you get that loan, whether you can enter a country, if you are a terrorist. The creators of algorithms assume that a faithful representation of who we are and what motivates us as individuals can be reconstructed by the careful analysis of data. They assume that their algorithms can reverse the flow of data, and reconstruct the individual. More worryingly this reconstructed representation is perhaps considered a more trustworthy representation of who we are, than who we say we are. This assumption, that our data speaks truth to who we are, is shared by numerous organisations, two of which that perhaps have the most

impact on your lives include the financial and security industry. The purpose of this research is two fold. The first is to investigate the construction of the algorithms and the datasets they process. The selection of data could determine the output of an algorithm before it is written, and the brittle nature of programming languages, and the algorithms they implement, may be ill-suited to the tasks to which they are applied. Secondly, there is a significant lack of transparency in the use of algorithms. We know almost nothing about how the algorithms are developed, and very little about where financial and security companies get the algorithms. We have begun the construction of a network database of security and financial organisations, and software companies and algorithms, in an attempt to unpick the some of the connections and relationships between these industries.

References:

Amoore, Louise & Piotukh, Volha Algorithmic Life: Calculative Devices in the Age of Big Data. Routledge; 2015.

Amoore, L. Security and the claim to privacy. International Political Sociology. 2014;8:108-112.

Harbisher, Ben De Monfort University
ben.harbisher@dmu.ac.uk

Public order, cyber security and surveillance

The following paper intends to examine emerging trends in protest management in the UK, looking predominantly at the November 5th demonstrations led by hacktivist collective Anonymous, and by associated campaign groups, all of whom maintain an active online profile. Owing to the repositioning of public protests under the remit of national security discourse, police are now able to situate such groups under the same operational framework as more severe threats to the nation, such as mass casualty acts of terror. While this in fact may not represent either their actions or their interests, it does allow demonstrators to become the target for Signals Intelligence (SIGINT), led by agencies such as the Joint Threat Analysis Centre (JTAC), and Joint Threat Research Intelligence Group (JTRIG), at GCHQ. Although this in itself is a fairly recent development, the increasing capabilities held by Britain's intelligence services for online surveillance has led to the reduction (if not) revocation of telecommunications provision for some protest groups, and the pre-emptive policing of many others. In the context of domestic SIGINT variants, Scotland Yard has its own Open Source Intelligence (OSINT) and Social Media Intelligence (SOCMINT) units, who regularly monitor social media channels belonging to campaign organisations. This is largely achieved via the use of complex algorithmic profiles searching for keywords, and via sentiment analysis tools – all targeted at social media content. Comparatively, groups such as JTAC and the JTRIG, are alleged to have used Denial of Service attacks against the Web Servers of suspicious organisations, and have conducted other covert Counter Intelligence Programmes (COINTELPROs) to deny, disrupt, degrade and deceive campaign groups they see as posing a threat to public safety, or to law and order. In this latter respect, it is the continual suspicion of wrongdoing, if not, the alleged threat posed by groups such as Occupy to trade and commerce in UK, that legitimises their surveillance. However, the question to be asked here does not equate to the mere fact of the matter, but to the relatively limited executive oversight, through which domestic spying campaigns are conducted under the pretence of national security.

Jordan, Tim University of Sussex
t.r.jordan@sussex.ac.uk

Mastering the Internet: Why does pervasive surveillance happen?

The fact of pervasive (if not total) surveillance based on automated information collection and algorithmic filtering is made clear by Snowden, Manning and Wikileaks evidence. How this occurs and the extent of it are of course important issues, however the question why governments through their security agencies conduct such surveillance also requires attention. Current arguments tend to move between the two poles of assumingsuch surveillance is bad because it is the basis of a totalitarian government and a bio-governmentality argument that builds on post-Foucauldian arguments about tracking populations. While both have something to contribute this paper will argue a necessary addition to understanding the drive to pervasive surveillance is to pay attention to the politics of information. Governments tend to have, often at the same time, two contradictory impulses toward flows of information: to restrictand censor or to collect and filter. The former is exemplified by national firewalls and direct censorship, such as China's constant deletion on Weibo, and the latter by such programs as Tempora and XKeyscore. This paper will argue that the latter can be understood as being propagated by new forms of information flow and thus not only as tools for government control and corporate profit but as tools that seek to engage all possible information about whole populations. These forms of information flow can be seen in three inter-locking principles: recursion, devices and networks and protocols. Recursion refers to ability of information outputs to be applied as inputs to the original process and so to produce exponential increases in amounts and types of information. Devices refers to the myriad 'black boxes' that are placed in information flows to manage the information overload recursion tends to produce. Networks and protocols refer to the two linked principles that organise recursions and devices into recurrent and stable patterns of information flow. Based on this kind of understanding of information flows, the desire to 'master the internet', articulated by the 'Five Eyes' security agencies, can be seen to be one that seeks the promotion and increase of information flows that then contribute increased forms of surveillance and, further, as dynamics inherent to current techno-cultures of information. The opposition of governments to encryption can also be understood in this light not only as seeking access to the meaning of communication but also to ensure all information is available for collection and filtering. While this paper will primarily deal with government and security agency approaches to surveillance and information, this argument will also be briefly related, through Deans' concept of communicative capitalism, to show how a similar dynamic operates in corporations.

Ju, Ran University of Illinois, Urbana-Champaign
ranju3@illinois.edu

The politics of algorithms: Sentiment analysis in civic deliberation in the US and Chinese social media

This study examines how algorithms can be deliberately designed to both facilitate and constrain civic deliberation in both American and Chinese social media platforms. Due

to the complexities of existing sociotechnical systems, both programmers and users can contribute to the design of algorithmic technology and use algorithms to reshape social arrangements in a well-structured community regardless of the preconditions. The purpose of this present study is to systematically examine the new challenges raised by sentiment analysis algorithms as compared to those that are already present in more traditional media analysis. Rather than proposing a way to get the algorithm under control to serve our rationally chosen ends, I am more interested in exploring how human or non-human actors are capable of acting and exerting agency into the process of sentiment analysis, and how the genres of algorithms themselves inscribe politics. My research will try to answer the question: Does the algorithm of sentiment analysis result a model that combines self-actualizing citizenship and self-perpetuating culture where civic deliberation is encouraged by personal identification and social recognition of personal life? Later this study will expand to broader issues regarding manipulation, surveillance and socio-cultural impact that the development of opinion-oriented information-access services gives rise to. A critical part of information-gathering algorithms is to find out what people think. With the growing availability and popularity of opinion-rich resources such as twitter and microblogging, new challenges arise as programmers now can and do actively use algorithm to seek out and understand the opinion of users. The underlying technology of sentiment analysis is based on a new type of Recursive Neural Network that builds on top of grammatical structures (Socher et al., 2015). I use the term “constitutive power” to demonstrate how cultural values and political aims can be achieved through the construction of algorithmic structures. By putting Actor-Network theory and Orlikowski’s extension of Giddens’ structurational model of technology into conversation, I then argue that the algorithm is both a chain, in which competences and actions are distributed and arbitrated, and an actor that retrieves its nonhuman agency in human common language.The constitutive power is inherent in the nature of algorithmic codes, and reinforced in the function of the interaction between technology and institutions. Users and algorithm tend to mutually shape each other, being aware of their interactions with the other. In the interaction process, there are no independently existing entities with their ontological separation. Algorithmic codes become speaking material fundamental to searching out the ways in which users might make sense of the constitutive force of discourse in their everyday communication. The algorithmic structure also uses the constitutive power that gives users to move against and beyond the very forces that shape their language and narratives. Here the constitutive power folded in the characteristics of algorithm acts on the user agency at two ways: first, algorithms make the user agency possible, the condition of its formative possibility within the online community; and second, it allows for user agency in the negotiation of its social impact in user’s own acting.

References:

Giddens A (1984) The Constitution of Society: Outline of the theory of structuration. CA: University of California Press.

Orlikowski W (2007) Sociomaterial Practices: Exploring Technology At Work. Organization Studies 28: 1435-1448.

Socher, R., Lin, C.C., Manning, C. and Ng, A.Y., 2011. Parsing natural scenes and natural language with recursive neural networks. In Proceedings of the 28th international conference on machine learning (ICML-11) (pp. 129-136).

Karatzogianni, Athina University of Leicester

Coopting the "Commons" is commonplace!

This paper discusses fieldwork research for the ESRC project 'The Common Good: Ethics and Rights in Cybersecurity-ERCS' in Barcelona, Paris, Berlin, Stockholm, St. Petersburg and New York. Twenty-five in-depth interviews with targeted activists, experts and practitioners were conducted between November 2015 and July 2016 across institutional, academic and activist settings. The research focuses on new algorithmic governance formations, particularly in the area of surveillance and cybersecurity. I draw from cyberconflict theory to map the interrelations across sociopolitical, ideological, organizational and digital elements influencing these formations (Karatzogianni, 2015, see also previous work). This paper discusses exclusively ideology and particularly the "commons" as a justification register for individuals and groups involved in alternative algorithmic governance, privacy advocacy and anti-surveillance resistance. I argue that this register is problematic in two critical ways. First, because the "commons" replaces capitalism's earlier "common good" as a justification register, i.e. the use of digital commons for ideological purposes, in the sense of Boltanski and Thévenot's (2006) economies of worth to reproduce inequalities, hierarchies and continuous labor exploitation (Karatzogianni, Matthews, Pucheu, 2016). Second, it does not produce a higher logical order of dissent, which surpasses capitalism as a social code. Platform cooperativism and other alternative models are explored and discussed with participants to ascertain whether they provide a strong alternative to current algorithmic governance able to overcome the quasi-totalitarian character of global trusted networks (corporate, governmental and third sector). These networks force the individual into an impossible hack or be hacked position of exclusion from digital planning (Karatzogianni and Gak). Yet, the securitization critique, although important, fails to account for opportunity structures, in which quieter forms of digital activism, such as platform cooperatives, blockchain activism and refugee hackathons, may well produce some answers to the problems algorithmic governance is currently facing.

References:

Boltanski, L. and Thévenot, L. (2006) *On Justification: Economies of Worth*. Trans. C.Porter. Princeton, NJ: Princeton University Press.

Karatzogianni, A. (2015) *Firebrand Waves of Digital Activism 1994–2014: The Rise and Spread of Hacktivism and Cyberconflict*, Basingstoke: Macmillan.

Karatzogianni, A., Matthews, J. and Pucheu, D. (2016) 'In the name of the collaborative economy: Digital intermediation platforms as a new material and ideological vanguard for capitalist expansion?' Easst Conference, Barcelona 2016.

Karatzogianni, A. and Gak, M. 'Hack or be Hacked: The Quasi-Totalitarianism of Global Trusted Networks', *New Formations: A Journal of Culture, Theory, Politics*, No.84/85 Societies of Control. Online available at: http://works.bepress.com/athina_karatzogianni/21

Lee, JeongHyun North Carolina State University
lee.ambrosia1205@gmail.com

There is no erasure: Politics in digital forgetting

The movie Eternal Sunshine of The Spotless Mind begins with a couple who just erase their memories of each other after breaking up. And the movie is filled with the process of erasing their memories. The starting point of this movie is an interesting imagination:

if we can erase our memories…In this paper, I want to drag this question into the digital. In California's Silicon Valley with other additional offices in the United States, the United Kingdom, and India, there is an eccentric company with millions of users from more than 100 countries. The company is called Reputation.com. The company is composed of engineers, researchers, and customer service staff, developing patented technology that helps online users to monitor, manage, and secure their information on the Internet. They fix negative or inaccurate search results damaging users' reputation and suppress unwanted materials on the Internet. Their job is not creating contents, but deleting it. Digital media have been a metaphor of preservation. After the digital, memories become digital in form. Based on its ever-increasing storage capacity and immediate processing, digital media have been developed toward storage media. Web 2.0 creates empty templates and we, as users, have obsessively filled the blanks on there. From our daily emails to social media contents, everyday life is inscribed in digital form. Due to that, we become the most documented beings who ever lived on the earth. Our past is captured and churned online. Now, our online presence is getting larger than our memories in mind and it is totally out of control. Search engines, such as Google, retain near perfect memories of what and how each one of us has used them, and collect our digital memories. Now, we often ask to delete and start to think about digital memories during our afterlife. In this context, I am asking about digital forgetting. With the growth of digital media, we have learned about how we use and fill the digital media; but we rarely learn or are concerned about deletion. Thus, this paper begins with the assertion that digital media is a storage medium, and, using software program "Vanish" as a case study, I trace an agent of digital forgetting by borrowing methodological insight from Latour's Actor-Network Theory. Vanish is a software program proposed by researchers at the University of Washington that seeks to protect the privacy of past and archived data. The main idea of the system is all copies of certain data in networked transmissions – emails, social media messages, documents on Google Docs, or photos on social media sites – become unreadable after a user-specified time. This system creates self-destructing data automatically after s user-specified expiration date, without any additional actions. In short, I constitute this paper in two parts: a short history of the newness of new storage media, and memory politics on digital forgetting. Borrowing methodological insight from Latour, I trace an agent of digital forgetting and define digital forgetting in digital storage media. I expect that revealing politics of digital forgetting ultimately raises security issues of our memories in algorithmic communication.

Leese, Matthias and Matzner, Tobias University of Tuebingen
matthias.leese@izew.uni-tuebingen.de
tobias.matzner@izew.uni-tuebingen.de

New knowledges, new problems: algorithmacy as threat reasoning

This paper argues that the central idea of securitization literature, threat reasoning, currently undergoes profound transformation through algorithmic security practices. What we call 'algorithmacy' establishes a new truth regime that builds on the promise of cognitive extension through the machinic capacities to reveal new insights about possible threats. However, with such new forms of knowledge come considerable epistemological and normative caveats. Throughout the paper, we outline the distinct human and machinic constructions of the world that regularly becomes subdued under

the frame of human terminology. We then engage the performativity of the algorithm, and the effects that algorithmic security practices unfold by producing highly idiosyncratic security subjectivities. Ultimately, we link algorithmacy back to the critical security studies agenda, thereby highlighting the importance of democratic principles in order to delimit algorithmic security practices in the first place.

Lehmann, Benedikt European Commission
Fellowbenedikt.lehmann@gmail.com

High-frequency trading and the technological constitution of anomie

High-frequency trading (henceforth, HFT) – a special kind of automated trading, which employs algorithms to execute orders in financial markets at speeds beyond human capabilities – can easily be thought of as an emergent sociotechnical practice. While the sociological literature on financial markets concentrates primarily on the mixed interaction between humans and machines, MacKenzie (2014) highlights the importance of understanding the emergence of HFT as the transition from an all-human ecology, to a mixed human-machine ecology, and increasingly to an all-machine ecology. The implications with regards to controlling, monitoring, and regulating markets are then significant. Namely, if the purpose of a sociological criminology is to analyse values of transgression and evaluate mechanisms of normative control, then the question arises which values are inscribed into algorithmic trading activities and how technological artefacts shape practices of control. This development in which computer algorithms increasingly take over for human voice trading reveals in an ironic twist the nature of agency, motivation, and more fundamentally, ideology in the contemporary stage of late-modern capitalism. In particular, cultural theorists, philosophers (see Fisher 2009) and even criminologists (see Hall and Winlow 2015) have begun to analyse human subjectivity in the form of post-political cynicism, which sees no desirable or feasible end to the capitalist mode of organising the economy. The principle step taken here is one away from the traditional Marxist conception of ideology as a mere constitutive naiveté, and towards a version of ideology which Zizek (1989) describes as being directly inscribed into the essence of the system. Automation by its very nature requires an understanding of the way in which technologies are ideologically inscribed and thus drive the way (transgressive) desire is organised. This paper will employ such an analysis of ideology to show how (automation) technology in financial markets is inscribed with the very values of an inherently transgressive capitalist system and constitutes the (sublime) object which promises capital accumulation beyond material possibility and transforms regulatory boundaries into barriers to be overcome. In this vein, (moral) regulation does not prohibit or limit (capitalist) desire, but frames the rules of the game and aids the (re-)constitution of a new kind of anomic subjectivity, which is detached from moral considerations.

References:

Fisher, M. (2009) *Capitalist Realism*. Hants: Zero Books.
Hall, S. and Winlow, S. (2015) *Revitalizing Criminological Theory: Towards a new ultra-realism*. London: Routledge.
MacKenzie, D. (2014) ‘A Sociology of Algorithms: High-Frequency Trading and the Shaping of Markets’, Unpublished Draft.
Zizek, S. (1989) *The Sublime Object of Ideology*. London: Verso.

Mangalousi, Dafni and Savvides, Leandros University of Leicester
dm344@le.ac.uk
ls326@le.ac.uk

Cyborg systems: discoursing the fourth industrial revolution at DAVOS and the EU

In the World Economic Forum (WEF) of Davos 2016 through its founder Klaus Schwab (2016) we were introduced to the upcoming Fourth Industrial Revolution where artificial intelligence, 3D printing, robots and quantum physics among other technological innovations, appear to lead technological development towards the organisation of life around cyber- physical systems. In other words, physical spaces such as cities, for example, are organised and governed through algorithmic communication while at the same time existing in a cyber-version of big data and smart applications. In this future, Haraway's (1991) cyborgs, "hybrid creatures composed of organisms and machines", epitomise the institutional tendency to transform biological organisms into metaphors about storing, moving, transforming and processing data and information. According to the European Commission, the E.U is a potential candidate to lead us towards the fourth industrial revolution (see Šefčovič, 2016) and it has been discursively working towards that for a couple of decades already. The discourse around the European Information Society (EIS) has, for instance, been previously used by the European Commission for the development and introduction of policies that perceive information and communication technologies as an opportunity for economic growth as well as a means for European governance; wherewith technology appears as "the solution to wider policy problems" (Shahin & Finger, 2009) and policy is understood "as a technologically driven phenomenon" (Gibbs, 2001, p.74). Most recently, 'Europe 2020' asserts a European strategy for smart, inclusive and sustainable growth and includes the so called Digital Agenda for Europe that, in response to WEF 2016, recently updated its website information to include the fourth industrial revolution term. According to David Noble (1984) "technological revolutions are not the same as social revolutions and are more likely, in our times, to be the opposite". In parallel with this line of thought, the fourth industrial revolution advocated at Davos and the EU, is by no means a social revolution. It is rather a technological one, which is, as we argue, an answer to the economic predicament and potential social upheaval. Once again, technology is communicated as spectacle (Debord, 1983) determining and predicting an upcoming revolution. Understanding the discourse around the fourth industrial revolution in connection to social and economic transformations in the E.U, we argue that the fourth industrial revolution, discursively represents the current reformulation of the European capitalist system as it attempts to overcome its systemic crises and remain competitive in the world markets.

References

Debord, G. (1983). Society of the spectacle. Detroit: Black & Red.
Digital Agenda for Europe (2016). The Fourth Industrial Revolution. Retrieved from https://ec.europa.eu/digital-agenda/en/fourth-industrial-revolution
Gibbs, D. (2001). Harnessing the information society? European Union policy and information and communication technologies.
European Urban and Regional Studies, 8 (1), 73-84.
Haraway, D.J. (1991). Simians, Cyborgs, and Women The Reinvention of Nature. London: Free Association Books.

Noble, D. (1984). Forces of Production; A Social History of Industrial Automation. New York: Knopf.
Šefčovič, M. (2016). Will Europe lead the fourth industrial revolution? Retrieved from www.weforum.org
Schwab, K. (2016). The Fourth Industrial Revolution: what it means, and how to respond. Retrieved from www.weforum.org
Shahin, J., & Finger, M. (2009). The history of a European information society: shifts from governments to governance.

Serafinelli, Elisa University of Sheffield
eli.serafinelli@gmail.com

Drone technology and visual ownership: Privacy and security issues

The use of various types of unmanned aircraft, popularly known as drones, has increased rapidly in recent years both for private leisure use and for commercial 'aerial work'. Drones are generally fitted with cameras and have the potential to change knowledge, visual experiences, and journalism. Videos of disasters, riots or other important events can be captured easily providing a wealth of information never seen before. Although the impressive potentialities the law surrounding drones is in limbo. Without a clear guide to using aerial drones, commercial drone use has effectively grounded bringing into account issues related to privacy and security. The contemporary surveillance studies (related to CCTV systems, for instance) need to be extended toward drone technology and the analysis of the ways in which mobile cameras are employed to collect and spread information. During an era where human life is mainly experienced online within networked systems the management of multimedia contents might go beyond users' own private purposes calling the urgency of revising the existing legislation that seems proceeding toward a general moral ambiguity. Previous surveillance studies (Lyon, 2001) emphasised the widespread general passive acceptance of the violation of privacy (given by the Internet and CCTV, for instance). Drone technology augments that phenomenon introducing the element of mobility, which represents an additional manifestation of the McLuhanian (1964) theorisation of media as extensions of man. Through a critical analysis of the artistic project Landed (Freeman's Wood) and the illustration of technological developments (Civic Drone Centre, University of Central Lancashire), this paper aims to unearth the existing conflicts between potentialities and risks concerning the public uses of drone technology. It aims also to discuss how advancements in drone technology alter the perception and experience of ubiquitous surveillance and privacy protection. The project Landed (Freeman's Wood) is an exploration of land-ownership and its significance for people and places. The project is focusing on a plot of land on the edge of Lancaster, known as Freeman's Wood, as an illustrative example through which the issue of land ownership can be explored. Storey G2 (art organisation directed by John Angus) commissioned artists (Layla Curtis, Goldin + Senneby, and Sans Facon) to lead an investigation of this plot, to research and explore land-ownership and its social effects, and to produce art works, which communicate and stimulate thought about these issues. This paper discusses in particular the work undertaken by the Civic Drone Centre in relation to the project as example of how artists can contribute to the understanding and dissemination of ideas around complex social and political issues, such as the ownership of the footage. It examines also ethical and moral issues behind drone use, seeks to

influence policy, and promotes interdisciplinary digital development. Conclusively, this paper presents the innovative transformations that the mediation and mobility of drones bring into the everyday human-technology interactions. Societies produce peculiar forms of information that are shaped by the co-presence of individual demands and the current typology of means of communication. Every alteration in the structure of societies has influence on individuals and means of expression creating crucial modifications within different environments such as business, leisure, art, privacy and surveillance. Lastly, it illustrates how the triangulation of mediation-mobility-visuality produced by drone technology radically transforms the visual perception of the world.

Reference List

Lyon D. (2001): Surveillance Society: Monitoring Everyday Life. Buckingham: Open University Press.

McLuhan M. (1964): Understanding Media. The Extensions of Man. London: Routledge & Kegan Paul.

Website reference: http://www.storeyg2.org.uk/

Tompsett, Brian University of Hull
B.C.Tompsett@hull.ac.uk

Ethical issues in security gamification

We have been used to computer security incidents being caused by faults in the computer system implementation and much research on computer security has focussed on technological improvements to the software, hardware and algorithms used. The trend is now for security incidents to be the result of human action and no technological changes or improvements could have mitigated or improved the security. One way of reducing the incidents of security failures is better user training. This works well for computer staff and some categories of employees but is not a satisfactory solution as members of the public and casual users are often exploited as part of a security attack. One method of educating and training users is gamification. Gamification involves simulating scenarios and rewarding the users for making the correct choice of action and warning them if they act incorrectly. The issue with Gamification is that it subjects members of the public to simulated attacks. This is where the ethical issues arise. Is it appropriate to expose general computer users to simulated attacks to improve their action in the event of a real security incident? Is it equivalent to a practice Fire Drill which most people may have experienced, or is it the equivalent of calling "Fire" in a crowded theatre?

Uldam, Julie Roskilde University
uldam@ruc.dk

Criminalisaton of radical political participation: Challenges to climate justice activism in social media

Radical political participation has been argued to constitute a key aspect of inclusive democratic societies by providing important critiques of government and corporate misconduct. Radical political participation in this view is understood as engagement with political and social issues, expressed in a variety of ways that do not always adhere

to traditional perceptions of parliamentarian politics (Mouffe, 2005). At the same time, responses to radical activism (from government, business, and the press) include discourses and practices that construct radical activists as thugs and criminals. In this presentation, I examine how these struggles are played out in social media, particularly how corporations work to vilify radical activists and how radical activists navigate an online arena with increasing surveillance. In doing so, I focus on the climate justice movement in the UK. Social media have been greeted as ground-breaking tools for affording greater possibilities for resistance, action and organisation by opening new terrains for groups excluded from the mainstream media to gain visibility (e.g., Carroll and Hackett, 2006; Kahn and Kellner, 2004). Critical perspectives remind us that as radical activists move from alternative media platforms to commercial social media platforms, they face increasing challenges in protecting their online security and privacy. This highlights the significance of the dual capacity of online visibility as government and business respond to radical activists as a potential risk. For governments, such risks are often construed in terms of national security (Deibert & Rohozinski, 2010; see also Pickerill, 2006). For corporations, they are construed as reputational risks (Bennett, 2003). This presentation explores visibility as a prerequisite and an obstacle to radical political participation. The dual capacity of visibility in social media enables both surveillance and countersurveillance by making not only the surveilled actor, but also the surveilling actor visible. It thus enables activists to monitor and expose corporate misconduct, but simultaneously renders them vulnerable to surveillance from corporations. Theoretically, it draws on Brighenti's (2010) and Thompson's (2005) (Foucauldian) conceptions of visibility and the idea that routinisation and invisibility creates asymmetry between those aware of the surveillance and those unaware of it. Empirically, it focuses on oil companies' surveillance of climate justice activists in social media and draws on files from BP on individual activists obtained through Subject Access Requests under the Data Protection Act. The files include email correspondence about surveillance of activists and a "Major Personality Report" with biographical information about individual activists. On the basis of this, I argue that particular practices of corporate surveillance of activists in social media contribute to criminalising and vilifying radical activists, broadly construing radical activism as illegitimate forms of political participation.

Wilmetts, Simon University of Hull
s.wilmetts@hull.ac.uk

Orwell 2020: Fictional metaphors of surveillance societies for a data-driven Age

Fiction plays a crucial role in shaping public attitudes towards surveillance. George Orwell's *1984*, for example, has a near omnipresent status in public, academic and practitioner debates about surveillance. Yet whilst surveillance studies experts widely acknowledge Orwell's influence, some argue that the metaphor of repressive state surveillance – Big Brother's boot stamping repeatedly on the face of humanity – is no longer fit for purpose. Instead they argue that more complex metaphors are required to account for the distributed and decentralised networks of relationships and systems of control that engender surveillance practices. Some argue that it is not "Big Brother" doing the watching, rather it us watching each other: "Sousveillance". Others argue that corporate surveillance by the likes of Facebook and Google poses a greater threat than even the NSA. Whilst still others propose a Deleuzian understanding of "Surveillant

Assemblages". All of these metaphors suggest the existence of a data-driven world that is far more complex than the one Orwell imagined. So if not Orwell, who can provide us with the fictional metaphors we need to understand the future trajectory of contemporary surveillance practices? This paper will focus on three recent novels, *The Circle, Super Sad True Love Story* and *Little Brother,* which have updated the twentieth century dystopian canon (Orwell-Huxley-Zamyatin) and arguably provided more appropriate guiding narratives for understanding our rapidly emerging "transparent society". This paper will explore these more recent dystopian representations of surveillance and suggest that a new canon of surveillance dystopias be assembled that is fit for purpose in the twenty first century.

Yang, Kenneth C.C. The University of Texas at El Paso **and Kang, Yowei,** Kainan University
CYANG@UTEP.EDU
KQUTEP@GMAIL.COM

Applying text mining software to analyze media contents about Edward Snowden in Taiwan and China

Edward Snowden's disclosure of National Security Agency's surveillance programs has a strong Asia tie. In May 2013, Snowden flew from Hawaii to Hong-Kong, SAR to leak classified information to two journalists, Glenn Greenwald and Laura Poitras, from the Guardian that later printed the news and it instantly became an international scandal. Some columnists from China have linked Edward Snowden's with then China's president, Chiang, to humiliate U.S. publicly. The event also has important implications to many Asian countries because the ongoing, incomplete, or failed democratization process in the region still has rampant government surveillance programs. For example, China was ranked in Freedom House's Freedom on the Net 2014 as one of three worst net freedom countries by allowing censorship of her citizen's Internet behaviors. China has also elevated its surveillance mechanism by requiring all Internet and mobile device users to register with their real names. In this paper, we plan to use textmining software to analyze media contents about Edward Snowden in three Asian regions to examine how news stories about national security, surveillance, and citizen privacy concerns were framed in the media. Specifically, we will use an ecological rhetorical analysis to see how political, social, and cultural factors affect the framing practices of Edward Snowden. The selection of China (an authoritarian country), Hong-Kong, SAR (a democratic society under the Chinese rule), and Taiwan (an island democratiC republic) presents a very interesting contrast to examine the dynamics between political systems, cultural similarities, and social differences in affecting the framing of Edward Snowden's images and behaviors in the age of algorithmic Communication.