6th Biannual conference of the Surveillance Studies Network

ABSTRACT BOOKLET

SURVEILLANCE: AMBIGUITIES AND ASYMMETRIES

Barcelona, 24th – 26th April 2014

13/03/2014

Draft version

ABSTRACTS

Introduction &Plenary Session

Surveillance Trends in the C21st

Session: INTRODUCTION & PLENARY SESSION

Date and time: 24th April 2014. (09:00-10:15h)

Authors: **Colin Bennett, Kevin Haggerty, David Lyon and Val Steeves**

A new book to be published in May 2014 outlines nine key surveillance trends in Canada and argues that together they exemplify the direction of surveillance development, within which specific emerging initiatives and innovations may be understood. Although the trends are the main focus, the most significant drivers of the trends and their consequences for privacy, social sorting and human rights are also detailed. The book arises from a major seven year collaborative research project and attempts to offer an accessible guide to surveillance in one country. This paper outlines the trends discussed and proposes that such an approach demonstrates the benefits of multi-disciplinary collaboration that also contributes to informed public debate and evidence-based policy change. The potential usefulness of documents like this for stimulating similar research in other countries — and thus also offering scope for international comparative analysis — is discussed, along with some suggestions about how such research programs could be mounted.

Big data

Big data and the ontology of media use: Theorizing the digital self in database economies

Session: **PARALLEL SESSION 1** – **Big data I**

Date and time: **24th April 2014. (10:30-12:00)**

Authors: **Göran Bolin and Jonas Andersson**

Intelligence on audiences in the age of the mass media was founded on representative statistical samples (surveys) or people meters, analyzed by statisticians at the market and research departments of media corporations. The techniques for aggregating data on media users in the age of pervasive and ubiquitous personal media (laptops, smartphones, but also credit cards/swipe cards and RFID), build on large aggregates of data analyzed by algorithms that transform data into commercial action. While the former built on sociological variables such as age, sex, ethnicity, education, and media preferences, the latter build on consumer choice, geographical position, Web movement, and pattern recognition (detection of non-representational correlations).

We need to ask which consequences this has for the ontology of the audience (as statistical, algorithmically generated aggregate) and the media user (as social subject). Based in qualitative research on media users (focus groups) this paper will discuss the implications of perpetual surveillance of the media user as a 'digital consumer' in public as well as private spaces, and how the 'digital self' produced by user movement in digital space gets increasingly separated from the social subject engaging in produsage through smartphones, tablet computers, kindles, and connected media use more generally. What are the changed perceptions of media users implicated by this increased knowledge change in data gathering for the media user him/herself? What consequences would this have for the perception of self as citizen and/or consumer? What are the consequences of geo-local surveillance for our thinking around public space? How does massive surveillance techniques impact on privacy concerns, as perceived by media users?

The Perils of Big Data

Session: **PARALLEL SESSION 1** – **Big data I**

Date and time: **24th April 2014. (10:30-12:00)**

Author: **Marc Kosciejew**

As Big Data begins to define and shape our times, it is crucial that we recognize and understand

not only its benefits but also its risks. Big Data presents many perils that may cause more harm than good. Handling Big Data responsibly and ethically requires knowledge and appreciation of its dark side: knowing the potential dangers will help us avoid or minimize them. This presentation aims to help shed light on major aspects of Big Data's dark side by discussing three of its major perils – to privacy, freedom, and agency – in order to provide a more balanced analysis of this feted phenomenon. As Big Data becomes increasingly more influential in countless aspects of life, society, and institutions, it is crucial to recognize, understand, and address these perils.

The Surveillance Dispositif of Cognitive Capitalism and Big Data

Session: **PARALLEL SESSION 1** – **Big data I**

Date and time: **24th April 2014. (10:30-12:00)**

Author: **Wook Inn Paik**

The issue on big data is in now on the mode. The practical approaches on big data are centered on how to make profit out of it. On the other hand the critical approaches emphasize the privacy problem and the advent of big (data) brother. This paper would concentrate on the formation of big data and appropriation of it by big internet service companies like Google and Facebook. They appropriate user generated contents and users activities by peer to peer production with their platform dispositif automatically.

The big companies appropriate the results of users activities and have monopolistic right on the big data. This paper will provide the analysis about the process of big data formation and the surplus appropriation by the big companies. The accumulated big data could be changed into the matrix for surveillance and profits for the big service platform companies. The Internet users' activities in SNS make "prosumer panopticon" which provides not only positive benefits for them but also new type of surveillance.

The purpose of this paper is to disclose the reason why the SNS platforms are new strategic apparatus for "participatory panopticon". Panoptic Surveillance based on bureaucratic dossier surveillance in Fordist stage had been transformed into electric database-based control since 1980s. The user participatory dispositif of web 2.0 has changed the method and range of social surveillance in 2000s. The coercion of Taylorite and "Orwellian Panopticon" was replaced by active consents of the Internet users. The new panopticon is constituted by prosumers' spontaneous coordination and self provision of their privacy data. The results of user activities in SNS were brought automatically into the big data system of the service providers in real time base. This

Internet-based surveillance based on positive benefits is the source of enterprise for them.

I would disclose the new method and characteristics of this p2p self panopticon from the perspective of big data. In this paper the relationship between SNS(Facebook, Twitter, Youtube) platforms and big data system of them would be analyzed.

Big Data, desymbolisation and the trivialisation of on-line surveillance

Session: **PARALLEL SESSION 2** – **Big data II**

Date and time: **24th April 2014. (13:00-14:30)**

Authors: **André Mondoux, Marc Ménard, Maude Bonenfant and Maxime Ouellet**

Big Data as data-capture phenomenon is an outgrowth of surveillance dynamics. It models present behaviours and, using algorithmic correlation, projects future behaviours. As a consequence Big Data is tied to a certain way of seeing the world (the Foucauldian episteme), that is, to an ideological position. Because it is incorporated right into data production tools and their circulation flows, Big Data is a technic whose ultimate purpose is its own operational capability: the more data Big Data amasses, the more Big Data frames the world as consisting of data, and so the more data there are for Big Data to amass. If we postulate that no world view can exist without symbolic mediation, it necessarily follows that an ideology loses legitimation (i.e., political/ideological coherence) if it is portrayed as merely a neutral, and therefore a “non-ideological”, technical operation. We might then justifiably ask how technical mediation by Big Data has come to supplant symbolic mediation, and how that legitimates the concomitant trivialisation of large-scale surveillance practices.

This paper examines Big Data in light of semiotics in an attempt to explain how digital data “transitioned” to a “desymbolised” status deemed neutral (i.e., non-ideological). Rather than reflecting some societal affinity for symbolisation, digital data are represented as merely the “natural” effect of a cause. Indices presented as neutral lie at the logical heart of Big Data. They “prove” that something no longer present once did “pass by”, leaving a wake. These trails, which became digital data the moment internauts moved through them, afford explicit proof of activities on line. It is the proliferation of such trails that feeds Big Data. Yet we shall show that these data are not assigned a value in any ethical sense. Instead, they are literally left “unassigned” after losing their original value. Once they find their way into the huge, unstructured databases of Big Data, they occupy the same level and acquire the same value. From desymbolisation to the closed world (Edwards 1996) of digital data, we move into a discussion of how the market resymbolises and

reassigns value to the whole world. Everything then takes on a commercial value that is no longer judged good or bad, but simply as marketable or not. In this vein we will analyse how Big Data technologies have been reduced to monitoring data trails. We will show that within its own operations, apart from their highly technical nature, Big Data embodies a sociohistorically identifiable ideology that disposes it to play a role in trivialising surveillance.

Mass surveillance technologies and the internal enemy

Session: **PARALLEL SESSION 2** – **Big data II**

Date and time: **24th April 2014. (13:00-14:30)**

Author: **Goupy Marie**

If the argument that technologies are neutral is now largely undermined, it yet remains singularly powerful in the political field. It is shown in particular by the various reactions following the recent revelations about the existence of a market of mass surveillance technologies mainly held by large European companies, allowing states like Libya, Bahrain, Syria, China, etc. to acquire technologies to monitor the entire population connected to the Internet. In this case, indeed, many managers of corporate communication, or even political authorities have then taken up the classic argument that companies are not responsible for the use that is made of their technologies. However, the operation of surveillance technologies reflects their inherently political nature: not only because companies comply with some requirements and precise requests from states, especially concerning intelligence, but even because in a deeper level these technologies and devices reflect a specific control system, a particular “économie de pouvoir” (Foucault).

Based on the study of manuals, brochures, presentation catalogues of surveillance technologies and processing intelligence sold by major high-tech companies, we would like to show that the operation of mass surveillance technologies has to be analyzed in its articulation with forms of more general strategies that are structured according to the idea of the internal enemy.

Big Data and the End of Practical Anonymity

Session: **PARALLEL SESSION 2** – **Big data II**

Date and time: **24th April 2014. (13:00-14:30)**

Authors: **Jason Derby and Ben Miller**

Given the increase in the analytical power of tools developed to sift through large data sets, the need for checks on indiscriminate data collection represent a new horizon for lawmakers, surveillance studies, and human rights. Work on de-anonymization of phone records to identify

location [1] or identity [2] and on movie selections to identify individuals [3] have shown that even coarse and imprecise information can be used to reattach user identifiable information to a particular person. Paul Ohm in “Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization” remarks that data can either be useful or perfectly anonymous[4]. Much as open government movements ended the episteme of practical obscurity, big data analytics is ending epistemic practical anonymity. Without robust checks on population level data collection, new analytical tools threaten to erase the legal and technical limits of traditional surveillance. Despite European data privacy laws, big data driven surveillance circumvents many existing boundaries and reveals the necessity for new regulatory frameworks to govern the linkable nature of data and its susceptibility to algorithmic interpretation. This paper considers the problem in four movements. First, it explains the impossibility of data anonymization. Second, it explores data linking with respect to the move to correlation and away from causation inherent in contemporary data mining practices. Third, it investigates the contemporary conflation of data and the human subject represented by that data as modeled by the historic substitution of the device for various aspects of the individual: i.e., if one assumes that a person is with their phone, knowing the device’s location is equivalent to knowing the person’s location. And lastly, we conclude this paper with suggestions for new regulations based on dilemmas posed by prior communication technologies.

1.Yves-Alexandre de Montjoye et al., “Unique in the Crowd: The Privacy Bounds of Human Mobility,” Scientific Reports 3, March 25, 2013.

2.Kumar Sharad and George Danezis, “De-anonymizing D4D Datasets,” accessed September 23, 2013, http://petsymposium.org/2013/papers/sharad-deanonymization.pdf.

3. A. Narayanan and V. Shmatikov, “Robust De-anonymization of Large Sparse Datasets,” in IEEE Symposium on Security and Privacy, 2008., 111–125.

4. Paul Ohm, “Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization,” UCLA Law Review, 57, 2010.

Sociology of big data and power: towards an anthropology of interconnections

Session: **PARALLEL SESSION 3** – **Big data III**

Date and time: **24th April 2014. (14:45-16:15)**

Author: **Sami Coll**

Big data seems to be the new coming golden mine of the information era. Many actors have high

expectations when others make high promises. But what is big data precisely? Is there one big data or several big data? Is big data a future, an ideal type or a myth? Is it the accomplishment of the surveillant assemblage that Haggerty and Ericson were describing more than 10 years ago and the forms of power that relies on the control of information?
One main issue about both the feasibility of big data and its potential to become a surveillance monster is its ability to develop interconnections. Interconnections between databases are what precisely make a surveillant assemblage more efficient. At the same time, data protection legislators are working hard to reduce these interconnections the most, mainly by the adoption of privacy principles: purpose, consent, security, disclosure, access, accountability (see EU legislation and ISO 29100). If these principles are respected, function creeps should be contained. But at the same time, big data relies on function creep. To put it clearly, without function creep, there is no big data.
In this paper, I would like to develop the understanding of this tension between the need of big data to allow interconnections to be flourishing and the mission of the legislator to contain these interconnections. Amongst other examples, I will show how some project aiming to use loyalty cards to regulate of public health cope with this tension. As a conclusion, I will argue that an anthropology of interconnections would be very useful to build a sociology of big data that could shed more light on the complex relationships between information and power.

Big data or dataveillance? The rise of the scientific enterprise and its social implications

Session: **PARALLEL SESSION 3** – **Big data III**

Date and time: **24th April 2014. (14:45-16:15)**

Author: **Sara Degli Esposti**

The so-called big data revolution is meant to transform organisations into social science laboratories where people's behaviour is investigated for targeted purposes. The new scientific enterprise is characterised by the use of sensors to track people and objects, the reliance on controlled experiments to identify causes and effects of targeted phenomena, and the translation of this scientifically gathered knowledge into actions meant to manipulate individual behaviour. While "big data", as rhetoric devise, it is used to make appear the increased volume, variety and velocity of creation of digital data as a natural, unavoidable fact, an analysis of the implicit assumptions and motives of the actors involved in fostering the big data phenomenon will unveil how dataveillance constitutes one of the most important and neglected driving mechanisms of the big data machine.

Dataveillance – which refers to the systematic monitoring of people or groups, by means of personal data systems, in order to regulate or govern their behaviour – helps us understand the socio-technical reality surrounding big data. In fact the big data debate, which is all about huge business opportunities and ICT investments, makes invisible the ethical and social implications of a future characterised by ubiquitous digital surveillance and automatic decision-making. Through an analysis of leading enterprises using big data applications to outperform competitors, the article will demonstrate the key role played by dataveillance and discuss how big data analytics is transforming social practices and human identities both in the workforce and in the consumer world.

How Data Mining Discriminates (or: Why Procedural Fairness Is Illusory)

Session: **PARALLEL SESSION 3** – **Big data III**

Date and time: **24th April 2014. (14:45-16:15)**

Author: **Solon Barocas**

Scholarship in surveillance studies has tended to oscillate between three rather different accounts of the discrimination effected by data mining (and social sorting, generally). First, scholars have argued that data mining may draw on criteria that are strongly correlated with those traits upon which certain groups have been unfairly discriminated against in the past—that is, to criteria that act as unintentional proxies for membership in a protected class. Second, scholars have stressed that data mining necessarily admits the possibility of inferential errors and that such errors may occur at systematically higher rates for members of already disadvantaged groups. Finally, scholars have also insisted that even accurate predictions can reinforce or exacerbate inequality. This presentation will consider recent computer science scholarship on non-discriminatory data mining that has revealed a number of unfortunate tensions between efforts that would address concerns with bias, error, and the perpetuation of inequality. It will explore the paradoxical finding that attempts to ensure procedural fairness may be in conflict with the imperative to ensure accurate determinations. And it will further explore why these results trouble the long-standing distinction between equality of opportunity and equality of outcome that grounds most anti-discrimination law.

CCTV

Public support and private disregard – CCTV and the competition between law enforcement agencies for the control of urban space

Session: **PARALLEL SESSION 1** – **CCTV I**

Date and time: **24th April 2014. (10:30-12:00)**

Author: **Francesca Menichelli**

Analyses of CCTV fall into three distinct, yet related, categories. Attention can either be focused on instances of targeted surveillance and the discriminatory potential of cameras, on how CCTV is used to police class borders in privatised public space, or on the globalisation of surveillance and of mechanisms of control within the "surveillance society". In contrast, this paper makes the case for an alternative understanding of surveillance cameras, that sees the competition between the different law enforcement agencies that operate in urban space as the main drive behind the diffusion of open-street CCTV systems. Based on fieldwork conducted in a medium-sized Italian city, the alternative paradigm that is proposed here challenges the narrative centred around the notion of the ever-growing securitisation of urban space and the accompanying assumption that ideas, strategies and techniques that originated in the English-speaking world will effortlessly reproduce in other – often radically different – contexts. Practically, understanding CCTV as one tool the local police can – and will – use in an attempt to defend their standing in their dealings with national police forces allows for a reconciliation of the apparent non-use of surveillance cameras on the part of police personnel with the enthusiasm with which CCTV is embraced by the force as a whole. On a more theoretical level, this is instrumental in highlighting how context-specific models of governance impact on cross-national phenomena such as the spread of open-street CCTV systems in ways previously unreported in the literature.

Privacy, data protection and ethical issues in advanced video surveillance archives search engines for security applications. The case of the ADVISE research project

Session: **PARALLEL SESSION 1** – **CCTV I**

Date and time: **24th April 2014. (10:30-12:00)**

Authors: **J. Peter Burgess and Dariusz Kloza**

The European Union co-funded research project ADVISE, or 'Advanced Video Surveillance archives search Engine for security applications' (2012-2015), aims at designing and developing a

unification framework for surveillance-footage archive systems in order to ease the work of law enforcement authorities in their fight against crime and terrorism. In other words, ADVISE aims at developing a tool for efficient evidence mining into multiple and heterogeneous video archives.

Both the research carried out in the ADVISE project and its final product raise privacy, data protection and other ethical concerns. The ADVISE project has committed to conduct research and to develop its output in a way that complies with European standards on privacy, data protection and ethics. This effort takes form on three levels. First, in order to comply with legal and ethical standards, the research consortium implements a strategy of privacy by design (PbD). Second, all research carried out by the project is subject to the scrutiny of an external Advisory Board and an internal data protection controller, among others. Third, in the implementation phase, having faced the question how to implement the PbD concept in the project, the research consortium chose a Privacy Impact Assessment (PIA) as a means of achieving this goal.

The research consortium has developed a tailored-down framework for assessing the impact on ethics, privacy and data protection of the ADVISE system and its components. According to this framework, any partner to the consortium that develops any element of the ADVISE system, be it a component or sub-system, as well as the consortium as a whole with regard to the whole ADVISE system, should carry out a PIA by providing answers to the PIA questionnaire and by applying recommendations found as an outcome of PIA process, before the component (sub-system, system) is developed. The same activity should be carried out when the specific element of ADVISE changes in a way that such a change can have an impact on ethics and/or on protection of privacy and personal data. The final PIA reports are monitored by the Advisory Board and other external bodies, if necessary.

This contribution will present how the ADVISE research consortium deals with privacy, data protection and ethical issues in its project. Firstly, having overviewed the project and its objectives, this paper will discuss the consortium's approach to the protection of privacy and personal data. In particular, it will explain rationale of choosing PIA, development of the PIA questionnaire and its revisions, conduct of PIA and implementation of its findings and recommendations. Secondly, having analysed the experience of performing PIA, it will provide observations and draw conclusion for the further stages of the project as well as for any similar research in the future.

On the limitations of 'smart' CCTV: technology, ethics and accountability

Session: **PARALLEL SESSION 1** – **CCTV I**

Date and time: **24th April 2014. (10:30-12:00)**

Authors: **Daniel Neyland and Patrick Murphy**

Recent years have been witness to a number of developments in what is often termed 'smart' (or algorithmic) CCTV. Alongside face recognition (and other biometric-based technologies) and gate recognition, object tracking, auto-deletion and access management systems have come to the fore as potential means to enhance the capabilities of surveillance systems. Questions have been raised about the potential of these technologies to invade privacy and expand the scope of surveillance on a new scale and in new ways. Simultaneously (although on a smaller scale) suggestions have been made that such developments might enable CCTV systems to be made more 'privacy sensitive,' through the deletion of footage, reducing the scope of visibility for video-based surveillance and increasing accountability through the provision of automated outputs on system activity. This paper reports on one such project which attempted to combine 'smart' CCTV developments in order to create a Privacy Enhancing Technology, assessed through a form of on-going Privacy Impact Assessment. The paper will suggest that such 'smart' developments can quickly run into significant and fundamental problems with technology, ethics and accountability. The paper will argue that the extent and deeply entangled nature of such problems can result in systems invading rather than enhancing privacy and becoming almost impossible to hold to account.

Surveillance and different aspects of trust in a low trust setting

Session: **PARALLEL SESSION 2** – **CCTV II**

Date and time: **24th April 2014. (13:00-14:30)**

Authors: **Fredrika Björklund, Ola Svenonius and Pawel Waszkiewicz**

In focus of this article is the interrelationship between the extent of trust in society and the presence of approving attitudes to measures of technological surveillance. It is fair to assume that strong systemic trust (trust towards the public and political institutions) make people more prone to accept state surveillance. If, on the other hand, trust is weak, people should hesitate towards an extension of the governments mandate to monitor and control the public. Scholars have recently put an interest in these issues but the results of the studies are ambiguous. The reason for that is probably that both variables – trust and surveillance – are rather amorphous. While leaving the concept of

surveillance aside, in this article we aim at an examination of the concept of trust and its potential bearing on attitudes to surveillance.

However, this study is framed within a specific political-historical setting – the low trust societies of former communist Eastern Europe. How can we investigate whether trust has any relevance for the current development of surveillance societies in this region? A first glance on the situation in these countries seems to overthrow the suggestion above. Low trust is often accompanied by a wide acceptance of government surveillance measures, or in other words: trust doesn't seem to have very much to do with attitudes to surveillance. But in order to get the full picture, we need to qualify the concept of trust in a way that makes it useful for the task. In this article we separate between three different aspects of trust: systemic trust and social trust – which is an established distinction in this context – and ontological trust (confidence). The last aspect alludes to the idea of reflexivity explored by for example Anthony Giddens and Ulrich Beck. We argue that this distinction and the examination of how these aspects relate to each other are essential for an appropriate study on trust and surveillance.

Closed Circuit Television Systems on Campus: A Study of Policies at Universities in the United States

Session: **PARALLEL SESSION 2** – **CCTV II**

Date and time: **24th April 2014. (13:00-14:30)**

Authors: **Thomas W. Lauer, Albert J. Meehan, Raymond Liedka and Roberta Michel**

Since 9/11 and particularly since the massacre at Virginia Tech University in 2007, many universities in the United States have begun installation of Closed Circuit Television (CCTV) systems on their campuses. What sorts of claims are being made about the use of these systems and what justifications are there for installing them? How might the pervasive use of monitoring technology affect traditional values associated with university life such as freedom of speech, freedom of assembly, privacy, and the freedom to explore? What policies are in place to ensure that whatever benefits associated with these systems justify both tangible and intangible costs? Over the past two years, we have analyzed university policies in the United States concerning the installation and operation of CCTV systems with the aim of gaining insight into these questions. For our study, we used the Carnegie database of universities and colleges. Our sampling criteria yielded 1361 universities that were four year not-for-profit institutions that excluded schools with a special focus, namely professional schools with a limited focus and service academies. We then employed a stratified random sampling procedure that resulted in a final sample of 370 schools.

We used a coding instrument for analyzing the corpus of policies in order to understand how the policies addressed such issues as: rationale or justification for CCTV usage, relevant personnel roles, public awareness, accountability measures, information security and data handling, routine operations of usage, and any relevant limiting measures.

One aspect of our study is to interpret the corpus of policies through the lens of Nissenbaum's contextual integrity which is concerned with examining the effects of new technological practices (such as the installation of CCTV systems) on one's expectation of privacy.

The Emergence of SMART CCTV in Scotland

Session: **PARALLEL SESSION 2** – **CCTV II**

Date and time: **24th April 2014. (13:00-14:30)**

Authors: **William Webster and Charles Leleux**

In the last few years, there has been increasing reference to the rise of SMART surveillance systems and specifically SMART CCTV (Closed-Circuit Television). Typically, these systems combine visual surveillance with computerised algorithms and networked technologies, in order to identify and track objects and predict patterns, for example human identification via face recognition and human behaviour via object tracking, profiling and analysis. They are perceived to be more 'intelligent' and consequently more effective than 'traditional' CCTV cameras and systems. However, whilst the emergence of these SMART technologies has gained a lot of attention, little is known about the actual deployment of such systems, their prevalence or technological capability. Moreover, it is also the case that there is no agreed definition about what constitutes 'SMART' CCTV and what distinguishes SMART CCTV from old-fashioned (and presumably 'dumb') CCTV. In the proposed paper, we will provide a critical analysis of the development of SMART CCTV in public places in Scotland. This will include; a review of published literature on SMART CCTV, including academic and practitioner materials; the development of a typology of SMART CCTV systems, to capture the different facets of smartness; an assessment of the driving forces behind the development of SMART CCTV; and, a reflection on the sematic use of the term 'smart', especially in relation to policy discourse and technological diffusion. The paper will also provide a first opportunity to report on a survey of SMART CCTV development by local authorities in Scotland. This survey is to be conduced in spring/summer 2013 and is designed to provide a 'factual' base-line of developments in the provision of SMART CCTV in Scotland. Greater knowledge about the development and diffusion of SMART CCTV will provide important insights

into the evolution of these technologies and the degree to which relevant regulatory and accountability mechanisms, public discourse and awareness, and the management of these systems are ‘in-tune’ with the speed of technological change.

Security

Exploring the Acceptance of Security Measures at Airports

Session: **PARALLEL SESSION 1** – **Security I**

Date and time: **24th April 2014. (10:30-12:00)**

Authors: **Gabriel Bartl and Lars Gerhold**

The focus of this contribution is set on flight passengers' perception and assessment of security measures at airports as specific areas of surveillance. The evaluation of acceptance and its conditions is rooted in the interdisciplinary research project SAFEST that deals with the prevention of mass panics (with a privacy-by-design approach) and area surveillance through a sensor-based system. In order to reflect the categories that constitute the attitudes of flight passengers towards such approaches to surveillance at airports, the development process of the technical system is accompanied by this study of acceptance.

The theoretical background of the study is to be found in the concept of "security culture" (Daase, 2012). This approach is based on the assumption that values and norms are constitutive elements for the handling of insecurity. For the evaluation of security measures at airports the conceptual framework serves as analytical tool in a way that these measures are considered as the operationalization and materialization of specific aspects of a „security culture". With the use of problem-centred interviews (Witzel & Reiter, 2000) the whole range of measures (camera surveillance, security staff, police, luggage scan etc.) was explored in terms of perceptional patterns and different modes of acceptance. All in all 18 interviews could be conducted at Airport Berlin, Schönefeld in September 2013.

Preliminary results show a general acceptance of security measures, even though the categories of the multifactorial construct of acceptance vary widely on the personal level. All in all different modes of acceptance could be observed that oscillate between informed consent and resignation. Besides, the perception of security measures seems to follow a logic of habituation.

Cyber-security: Between Tech-fixes and Biopolitics. Individual Security in a Digital Age

Session: **PARALLEL SESSION 1** – **Security I**

Date and time: **24th April 2014. (10:30-12:00)**

Authors: **Katja Lindskov, Jacobsen and Rune Saugmann Andersen**

A set of concerns related to the integrity and safety of the individual arguably arises from modern states' practices of database creation and information sharing. Although these practices are nominally carried out to enhance state security, this paper explores how such practices may, however, entail the emergence of new risks to individual security. Specifically, the paper argues that in modern state practice, especially since the 9/11 attacks, the practice of data sharing has side-stepped individual privacy and security concerns as state security (terrorism) and biopolitical management of populations (immigration) have taken precedent.

Based on an analysis of cyber security discourse, the paper argues that the dominant rendering of cyber-security as a question of technological reliability and the ability to keep databases and systems 'secure' from alien intruders with malign intentions relies on a state-centric and managerial security concept. The paper contrasts this discursive rendering of cyber-security with a view of data as enmeshed in material semiotic assemblages where the meaning of any data or data stream is not predetermined but emerges as a relational effect of the network it participates in, i.e. through the practice it is engaged in.

This perspective highlights how privacy assurances and security threats emerge retrospectively as a result of network use rather than as the result of a calculated, pre-determined balancing act (Walker). When viewed from the perspective of security concerns of individuals, threats identified in dominant cyber-security discourse thus cannot be compared ex ante to risks, and outside intrusion cannot be seen as the only 'threat' to data. Rather a host of ethical questions emanates from state practices including the merging of databases, profiling and categorization of individuals based on scattered electronic traits of behaviour, and the automatic bracketing of the rights of individuals based on this automatized profiling.

Bringing to the fore the discrepancy between recent critical thinking on cyber-security (Deibert 2010; Hansen & Nissenbaum 2009) and the individual security concerns emanating from digital databases, the article concludes that the academic field needs to pay closer attention to what is meant by cyber-security, rather than treating it as an un-political concept.

Electronic surveillance

Session: **PARALLEL SESSION 1** – **Security I**

Date and time: **24th April 2014. (10:30-12:00)**

Author: **Laura Plana García**

School children are subject to increasingly sophisticated and pervasive forms of surveillance from parents, school authorities, the state and others. This includes school authorities monitoring school children's social media use and parents using geo-location devices to track their children's whereabouts. While surveillance is generally justified with considerations of safety, security and discipline, such surveillance may have detrimental effect on the social and personal development of school children. This presentation will enquire into this new threat to children's privacy and investigate the legal framework in which such surveillance activities take place.

Surveillance of Environment Movements in Canada: Critical Infrastructure Protection Threats in the Era of the Petro State

Session: **PARALLEL SESSION 2** – **Security II**

Date and time: **24th April 2014. (13:00-14:30)**

Autors: **Jeffrey Monaghan and Kevin Walby**

Surveillance practices targeting environment movements have become increasingly normalized across Canada. While security discourses related to 'eco-terrorism' have evolved over the past three decades, the current socio-economic milieu – characterized by a convergence of post-9/11 security governance regimes and a booming extractive energy economy – has profoundly impacted the way that environment movements are categorized as national security threats. Contributing to literature on surveillance studies and social movement suppression, we detail how the trope of 'critical infrastructure protection' (CIP) enabled the normalization of surveillance targeting environment movements in Canada as well as enhanced the surveillance capacity of key federal security and policing agencies. Our article explores data that underline two significant developments: 1) we analyze public documents and bureaucratic shifts demonstrating the growth of CIP as a discursive and material site for security enhancement and the changing character of CIP as a security field, from Cold War bi-polarities to Global War on Terror asymmetries; 2) we examine secret documents released through Access to Information requests that demonstrate the normalized categorization of environment movements in Canada as national security threats. We conclude with reflections on the link between national security classification / categorization and the

surveillance capacity of state agencies.

Acceptable surveillance-oriented security technologies: insights from the SurPRISE Project

Session: **PARALLEL SESSION 2** – **Security II**

Date and time: **24th April 2014. (13:00-14:30)**

Authors: **Sara Degli Esposti and Elvira Santiago**

Pre-emptive security emphasizes the necessity of envisioning and designing technologies enabling the anticipation and management of emergent risks threatening human and public security. Surveillance functionalities are embedded in the design of these technologies to allow constant monitoring, preparedness and prevention. Yet surveillance-oriented security technologies, such as smart CCTVs or Deep Packet Inspection, bring along with their implementation other risks, such as risks of privacy infringement, discrimination, misuse, abuse, or errors, which have often triggered public outrage and resistance. The same measures meant to foster human security, can potentially make people feel insecure, vulnerable, and exposed. This outcome is the result of a narrow approach toward problem solving that does not take into account those same people the technology is supposed to protect. Drawing from both the socio-cultural and psychometric approaches to risk analysis and from the literature on public engagement in science and technology, this article presents a new methodological tool, which combines traditional citizen summit method with an innovative mixed-method research design. The objective of this new form of participatory exercise is to engage the public and gather socially robust and in context knowledge about the public acceptability of these technologies. The method has been developed as part of the SurPRISE project, funded by the European Commission under the Seventh Framework Program. The article presents the theoretical framework and preliminary results of citizen summits organized across Europe.

Regulating surveillance oriented security technologies: social and political consequences of the pre- emptive surveillance in Europe

Session: **PARALLEL SESSION 2** – **Security II**

Date and time: **24th April 2014. (13:00-14:30)**

Authors: **Vincenzo Pavone, Elviara Santiago**

Over the past twenty years, the concepts of security and surveillance have undergone multiple and

often contrasting reformulations, shifting from an emphasis on territorial integrity and national sovereignty to a new focus on human security and development and, after 9/11, back again to a new concept of statehood based on homeland security and war on terror supported by new ways of surveillance technologically oriented. In this new approach to security and surveillance, the priority seems to have been reassigned to territorial integrity, yet with a new emphasis on pre-emptive action, anticipation of threats and risk management. In this controversial trajectory, the roles played by the shifting nature of global security threats and the national reactions to terrorism and transnational organized crime have been largely studied. Yet, little work has been done on the role played by the massive and often indiscriminate development and deployment of surveillance-oriented security technologies and their consequences for our democracies. In fact, there seems to exist a mutually constitutive relationship by current concepts of statehood, pre-emptive security and surveillance-oriented security technologies. Through discourse and frame analysis of the most recent EU and national security strategy documents, we show how security is an expanding concept related to pre-emptive actions and threat anticipation to be achieved by the use of new controversial surveillance technologies. In this new context, monitored citizens, thus, are asked to renounce to part of their liberty in exchange for an increased level of security. However, if citizens cannot be free unless they are safe, they also cannot be safe unless they are free, or they would no longer be citizens.

Security, Vigilance and Citizen Surveillance

Session: **PARALLEL SESSION 3** – **Security III**

Date and time: **24th April 2014. (14:45-16:15)**

Author: **Kerrin-Sina Arfsten**

Since the attacks on September 11th, 2001, the creation and mobilization of a well-informed, proactive and vigilant public has become one of the hallmarks of the U.S.'s homeland defense strategy. Every citizen is asked to assist the state in its task of identifying and capturing potential 'terrorists' in order to prevent them from carrying out future attacks. The citizen is to do this by acting as the 'eyes and ears' of law enforcement, by staying alert and watchful, and by reporting any unusual or suspicious objects, people and circumstances to the authorities. The government's message is reinforced by a number of government programs and visual media advertising campaigns like the so-called "If you see something, say something" security awareness campaign. Drawing on qualitative data collected for my Ph.D. project, this paper explores the "If you see

something, say something" public vigilance campaign. The first part of this paper examines how public vigilance in the post-9/11 era is collectively constructed through the campaign and employed as a technology of security government that structures certain fields of visibility, engages the affective and frames specific subjectivities. The second part then analyzes how this vigilant mode of governance is contested, challenged and subverted, for example through artistic interventions. Together the two parts shine light on the role public vigilance campaigns play within the larger framework of social control in late modern society.

Assessing the Impact of Security Technologies on Security: Technology and the Co-Production of Order by Ambiguity

Session: **PARALLEL SESSION 3** – **Security III**

Date and time: **24th April 2014. (14:45-16:15)**

Author: **Lars Ostermeier**

Assessing the impact of security technologies on security raises questions about how security is understood and how technologies are thought to relate to security. Except for CCTV technologies, only a very small numbers of studies in this regards is available. Drawing on a number of interviews with security technology experts in mass transport systems in Israel, Italy and Germany, the paper discusses three different narratives that are used to construct the notion of a positive impact of security technologies on security. It is argued that these narratives provide for different ways of managing the ambiguity of security technologies, thereby helping to co-produce the social order that inscribed to the technologies. In the first narrative, security is a contested concept and the impact of a technology on security remains vague. In the second narrative, security has been defined as an 'adequate' problem and the impact of a technology can be 'clearly' assessed. In the third narrative, a security problem is being constructed in order to provide a use-case for a technological solution. This analysis provides a contribution for the development of methodologies to assess the impact of security technologies on security. The narratives show how a certain way of assessing the impact of a technology on security becomes dominant. A special emphasis is made on the role of ambiguity in these narratives.

The Law of Diminishing Returns as guiding principle in interpreting Article 8 of the European Convention on Human Rights, a proposal

Session: **PARALLEL SESSION 3** – **Security III**

Date and time: **24th April 2014. (14:45-16:15)**

Author: **Rozemarijn van der Hilst**

In discussions on surveillance for the purpose of counter-terrorism, the debate is often phrased as privacy versus security and the need to strike a balance. Scholars have criticized the use of the image of a balance in this context, because it promotes a narrow understanding of the two key concepts at stake, and misrepresents the relationship between the two. Despite the scholarly criticisms, the European Court of Human Rights upholds this paradigm in their case law on Article 8 in relation to the use of counter terrorism technologies.

In order to reframe the debate and inform the Court's decisions, I propose to abandon the image of the balance and instead use the (economic) law of diminishing returns as guiding principle in deciding to what extent the right to privacy should and can be limited with the view to increase security. In applying the law of diminishing returns, the relationship between privacy and security can be more accurately portrayed. Firstly, it allows for a broader approach to the notions of privacy and security, wherein the protection of privacy is seen as an integral part of security and it is recognized that security is construed both factually and subjectively. Secondly, the law of diminishing returns is better equipped to take into account potential 'side-effects' that the use of counter terrorism may have on overall security, because it demonstrates that the relationship between privacy and security is dynamic, rather than 'static' as the image of the balance would suggest.

Communication

A tale of the three wise monkeys: patterns of legitimization in surveillance scandals

Session: **PARALLEL SESSION 1** – **Communication I**

Date and time: **24th April 2014. (10:30-12:00)**

Author: **Matthias Schulze**

Currently, we are witnessing yet another surveillance scandal. Since the leaks by Edward Snowden, the public sphere has been aware of the NSA's total surveillance practices regarding Internet traffic. While the scale and dimension of this surveillance program is definitely new and unmatched by anything before, the public debate and political reactions to it are not that innovative. In fact, the political response in Western governments is (mostly) unitarily to downplay the leaks, reject their implications and scale of the leaks, and to discredit whistleblowers or the criticism as "anti-Americanism" or being "unpatriotic", just like in previous scandals.
The aim of this paper is to analyze legitimization patterns regarding different surveillance practices in Western Democracies. What are the relevant features of the justification discourse? What kind of threats are constructed to justify the measures? What is the role of misinformation and denial of evidence? The argument is that political responses employed by (mostly conservative) governments share discoursive patterns, strategies and metaphors and resemble a distinctive narrative of surveillance justification. Typically, surveillance measures are introduced via securitization speech-acts (Buzan and Wæver 1998), where a threat is constructed to legitimize the implementation of extraordinary measures in the light of an essential threat. By that, a former political, democratic and thus transparent process is lifted into the realm of security and secrecy, legitimizing security measures that otherwise would not pass the democratic deliberation process. The basic narrative is "if we do not quickly establish this particular security measure because of threat X, something will happen". Therefore, secrecy is needed and transparency and democratic control risks the success of the measure. However, if surveillance programs are leaked, they itself become perceived as threats by the general public and their former legitimation is in question. To prevent their dismantling, justification narratives are established by political officials to defend the extraordinary rights. Therefore securitization speech acts are adapted. A common trope is the denial of its extraordinary character and the reframing as something normal, necessary and not even total at all. The former extraordinary measure is rhetorically de-securitized. This is in sharp contrast to the rhetorics that introduced the surveillance tools earlier and resembles the

normalization of the exception (Bigo 2002, Hall 2007). It resembles the Japanese tale of the three wise monkeys which do not see, hear or speak

Several surveillance scandals will be analyzed, starting in 1989 when “Der Spiegel” published leaked information about the NSA’s surveillance program back in the day. In 1998 the European Parliaments debated about Echelon System and possibilities of industrial espionage in the light of global telephone wiretapping by the NSA. In 2005 the “New York Times” reported NSA wiretapping activities which sparked the debate. To enhance the explanatory power of this approach, most-dissimilar cases are analyzed for the same kinds of patterns: surveillance forerunners like Great Britain and the USA, and privacy advocates like Sweden and Germany. It is argued, irrespective of which country a security measure is employed in, the narrative of surveillance justification is similar.

The End of the ‘Noble Lie’: Sousveillance and Other Forms of Parrhesiastic Resistance to Contemporary Biopolitics of Information and Communications

Session: **PARALLEL SESSION 1** – **Communication I**

Date and time: **24th April 2014. (10:30-12:00)**

Author: **Miguelángel Verde Garrido**

Contemporary society is global and digital. States and corporations extend their political and economic power into digitality by means of the formulation and articulation of global and national security, surveillance, and censorship policies and practices concerned with information and communications technologies (ICTs) infrastructure, networks, and content.

States and corporations control most mechanisms of production and circulation of information, establishing a political economy of truth that is vital for economic production and political power. States and corporations deploy legislations, disciplinary and panoptical policies and practices, and apparatuses of security concerned with information and communications. These deployments synergize into a biopolitics of information and communications – i.e., a normalization of civil societies’ political and economic agency, inasmuch citizens and consumers, which makes difficult to contest state and corporate régimes of truth.

The speedy development and economical accessibility of novel ICTs remarkably strengthen civil societies’ demands for more transparent and accountable information about state and corporate actions, and enhance the former’s sousveillance of the latter. Whereas demands for transparency and accountability are not new to civil society, when sousveillant, they can be understood either as a contemporary inversion of disciplinary panopticism or, even, as the deployment of disciplinary technologies of power by civil society.

Collective hacktivism and whistle-blowing are sometimes crowdsourced research and data mining endeavors that attempt to produce and circulate information. These efforts can be understood as sousveillant and parrhesiastic contestations of state and corporate régimes of truth. Anonymized/encrypted communications and social media allow for collaborative networks that enable an ever more recurrent periodicity of parrhesiastic discourses relevant to national and global politics.

Contemporary biopolitics of information and communication require that civil societies be not only responsibility for their political agency, but also for the resemantization of their own politics of truth and, by extension, of their newborn digital agency.

Communications Surveillance: Problematic for Whom?

Session: **PARALLEL SESSION 1** – **Communication I**

Date and time: **24th April 2014. (10:30-12:00)**

Author: **Wil Chivers**

This paper reports on empirical research examining the construction of online and communications surveillance as a social problem. Employing a social constructionist perspective and drawing on the work of Cohen (1972) and Gusfield (1981), the research identifies the claims-makers who advocate or oppose changes to communications surveillance practices in the UK and examines the nature of their claims. These competing dialogues are used to draw out suggestions as to the nature of the interaction between online surveillance practices and counter-measures aimed at resisting them.

Drawing on empirical data from a discourse analysis of the publication, consultation and response to the UK Draft Communications Data Bill (2012), it is suggested that legislative changes have the potential to act as a catalyst for greater public understanding of online surveillance and consequently to mobilise public attitudes against such proposed technological developments. Placing this analysis in the context of more recent revelations concerning the extensive electronic surveillance capabilities of UK and US intelligence agencies, the paper concludes that, while the recent history of online and communications surveillance provides strong support for the perceived asymmetry of surveillance power relations, this history also points in the direction of measures which have the potential to level the surveillance playing field.

Representations of Surveillance in Estonian media (Case Study of reception of PRISM)

Session: **PARALLEL SESSION 2** – **Communication II**

Date and time: **24th April 2014. (13:00-14:30)**

Authors: **Andreas Ventsel and Mari-Liis Madisson**

The aim of this paper is to explicate how the leakages concerning details of top-secret United States government mass surveillance program PRISM were contextualized in Estonian public informational space. This topic addresses even people who are normally distant form politics because it touches the cornerstone of contemporary identities: the right for free internet. Internet is quite often connected with the revolutionary potential of increasing direct democracy and two-way communication between citizens and the state. That kind of cyber-democracy discourse has an important role and strong axiological values in Estonian public identity.

Our preliminary observation indicated that in representations focusing on the leakages of Snowden, there dominates the discourse of fear. In the viewpoint of cultural semiotics the collective fear activates a specific logic of generating associations; and it transforms significantly already existing structures of meaning. People fear that the general cornerstones of democracy (e.g. freedom of speech; supremacy of law; freedom of the press etc) are questioned. In the atmosphere of fear and uncertainty, the communicational mechanisms, normally oriented to outward communication, tend to transform and start to produce hermetic explanations and tend to contextualize the event by the analogies of cultural memory.

By analyzing above described reception of PRISM we would like to focus on two intertwined aspects: 1) map the main ways of articulating the scandal; 2) explicate the inner-logic of those rhetorical tendencies in the point of view of cultural semiotics, cultural studies and discourse analysis. We think that this approach provides a possible basis for predicting how interpretational frameworks can affect auditorium`s willingness for new connections (dialog) or self-absorption (polarization, hermetic meaning-creation when the cultivation of previously existing connections is taking place).

In order to understand how PRISM scandal is understood in Estonian public informational space, we will conduct a qualitative survey of rhetoric of online-publications.

In the (cybernetic) loop: Public service as a counterpoint to surveillant management of media audiences

Session: **PARALLEL SESSION 2** – **Communication II**

Date and time: **24th April 2014. (13:00-14:30)**

Author: **Jonas Andersson Schwarz**

In an era of ubiquitous digital media distribution – where real-time monitoring, measurement, and algorithmic prediction are features inherent to the very delivery platforms for audiovisual content – how does Public Service Broadcasting (PSB) respond to this condition?

Among commercial broadcasters, predicting audience preferences by means of automated monitoring and data retention is becoming increasingly common, especially in so-called 'on-demand' services such as Netflix. Largely, innovation in the interrelated spheres of media production, distribution, and consumption seem to rely on surveillant practices. Further, broadcasters see a related problem to do with organizational autonomy, as they have to rely on external actors such as Google, Apple, and Facebook in order to gain reach and efficacy.

Sweden is a leading country not only in domestic internet connectivity but in file sharing and innovative media distribution as well (Pirate Bay, Spotify), alongside a very strong PSB tradition. Its PSB remit and operations are currently being overhauled, with computer ownership now being associated with having the ability to receive audiovisual broadcast media – thus making it compulsory to pay a PSB license fee if merely owning a computer.

It is pertinent to explore the ethical and political consequences of this new mode of broadcasting. Although some of this research remains somewhat speculative, it is advisable that explorative research is conducted in order to better anticipate policy and regulation.

Empirical results from interviews with Swedish PSB executives and managers will be analyzed, in order to devise a theory on the incentives and real-term possibilities of algorithmic audience prediction and maximization, and how different forms of 'panspectric' mass-surveillance make possible an ethics and regulation that can be either paternalistic or insouciant as to what the audience is thought to need and want. A possibility for a 'benign' panspectrocism (a more democratically accountable data and innovation management) will be proposed.

From porn to cybersecurity passing by copyright: How mass surveillance techniques are gaining legitimacy despite public outcry…

Session: **PARALLEL SESSION 2** – **Communication II**

Date and time: **24th April 2014. (13:00-14:30)**

Author: **Sophie Stalla-Bourdillon**

In its recent joint communication the European Commission defines the term of cybesecurity in the following manner: "[c]yber-security commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber-security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein" . It is added that "[c]ybersecurity efforts in the EU also involve the cyberdefence dimension . To increase the resilience of the communication and information systems supporting Member States' defence and national security interests, cyberdefence capability development should concentrate on detection, response and recovery from sophisticated cyber threats". The European Commission notes that threats can have different causes and in particular that threats are not necessarily linked to the commission of crimes: "Cybersecurity incidents, be it intentional or accidental, are increasing at an alarming pace and could disrupt the supply of essential services we take for granted such as water, healthcare, electricity or mobile services. Threats can have different origins —including criminal, politically motivated, terrorist or state-sponsored attacks as well as natural disasters and unintentional mistakes".

Notably private and not public actors are meant to have a leading role in the promotion of cybersecurity, despite its large scope. In its joint communication the European Commission has indeed asked the industry to "take leadership in investing in a high level of cybersecurity and develop best practices and information sharing at sector level and with public authorities with the view of ensuring a strong and effective protection of assets and individuals, in particular through public-private partnership" . Non-governmental actors being essentially commercial entities are therefore officially conceived as privileged partners of Member states and the Europe Union. Does it mean that these privileged partners should be allowed to use special means and in particular mass surveillance techniques to ensure cybersecurity?

Indeed, the technology developed and implemented by the industry to prevent and monitor threats to network security has in several cases serious repercussions for Internet users, in particular in terms of privacy, amounting de facto to the generalisation of mass surveillance techniques. It is

thus crucial to identify the implications of the technology being developed in order to make sure adequate safeguards, namely legal safeguards are complied with. This is all the more true that in various cases it has proved very difficult to apply existing legal rules in a well-informed way. The legal confinement of Deep Packet Inspection (DPI) technology shows it perfectly.

The aim of this paper is thus twofold. First, the author shows that despite the increasing public awareness in relation to the capabilities of Internet service providers (ISPs), which has had the consequence of reducing the popularity of DPI technology among IPs and thereby its overall use in 2012, a cross-field examination shows that DPI technology is in fact progressively gaining legal legitimacy as a tool of mass surveillance for the purpose of guaranteeing information security. Second the author stresses the need to rethink the liability regimes of Internet intermediaries and in particular ISPs which have "traditionally" been conceived as mere passive intermediaries. If ISPs, among others, have to "take leadership in investing in a high level of cybersecurity", after having been called upon in the fight against child pornography and online copyright piracy, it is clearly doubtful whether mass surveillance techniques such as DPI will progressively disappear or become outdated. As a result, the horizontal regime of exemptions of liability set up by the Directive on e-commerce and grounded on the assumption that these providers' activity "is of a mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored" should be balanced with duties to use invasive technologies for an effectively restrained number of purposes and the setting up of mechanisms to prevent the creeping extension of self-regulation.

Fiction

The Specter of Surveillance in Postwar American Literary Expatriate Paris

Session: **PARALLEL SESSION 2** – **Fiction I**

Date and time: **24th April 2014. (13:00-14:30)**

Author: **Craig Lanier Allen**

"Exile is like unrequited love. Ours was a sick nation in those terrible days. I left my native land because I couldn't stand watching the rape of justice and the murder of decency. I left America because the alternative to leaving was suicide or madness." (Harold L. Humes, 1963; Co-Founder of the Paris Review).

Within the storied history of American expatriatism in Paris, writers of the Post-WWII period (1950 to 1960) represented a substantive and stylistic rupture from the generations of American writers, artists and intellectuals who preceded them and those who would arrive in Paris after them. This rupture consisted mainly in the politicization of these American literary expats in terms of both the motivations behind their decisions to leave the United States and the more explicitly political content of their literary and artistic production.

The end of WWII gave rise to American geopolitical primacy and an American desire for a return to domestic stability and tranquility. The postwar American artists, writers and intellectuals who made their way to Paris were by-in-large skeptical of the presumed saliency of American power and sensitive to the price the pursuit of American social tranquility was exacting from their artistic freedom. Beyond this notion, the particularities of each expatriate's political motivations were nearly as varied as their numbers. Correspondingly postwar American writers in Paris must be considered as an amalgamation of separate and distinct artistic and political communities rather than a single cohesive group. The black American writer Richard Wright (Native Son, 1942; Black Boy, 1945) and George Plimpton, a quintessentially New England WASP and founder of the Paris Review, presided over two of the most important American literary circles in Paris. These circles were notably different in terms of their cultural production and the politics of their members.

The group of postwar African American literary expatriates has become collectively referred to as Paris' Rive Noire (Black Bank), and was treated by the American government as a kind of antagonistic black American brain trust-in-exile. As such, its members—writers like Wright, James Baldwin, and Chester Himes—came under the active suspicion of those charged with safeguarding American interests against the explicit critique of black expatriate writings and the implicit critique of

their exile. In contrast, the founders of the Paris Review presented American national security policy formulators with a potential ally in the American cultural Cold War. This environment presented opportunities for the American government to monitor, report on and influence individual American expatriates or their groups deemed to pose a threat to American national security interests.

Surveillance—the surreptitious observation and gathering of information about a subject—is the essential practice upon and around which spycraft, or intelligence collection , is based. A specter of surveillance emerged within both the everyday lives and literature of the postwar American literary expatriate community in Paris. This specter of surveillance consisted of a pervasive, existential understanding among these American writers that their actions were being observed and reported on by various American intelligence agencies in Paris. Most important with regard to American literary history, this specter of surveillance served as an expression of postwar American expatriate anxieties in response to both real and imagined surveillances. Correspondingly this specter of surveillance became a defining contour of Rive Noire narratives and the history of the Paris Review's founding, serving alternatively as device, motivation and backdrop for much of the fiction and non-fiction the writers produced.

This paper will explore the cultural geography of American expatriate literary circles in postwar Paris with regard to the specter of surveillance. I will identify the postwar Parisian places central to the Paris Review's founding and locate the dimensions of the specter of surveillance within its location-specific ephemera. In so doing I will demonstrate the material connection between post- and Cold War American national security interests and the choices made by members of the Rive Noire and the founders of the Paris Review, respectively. Last, I will argue for considerations of the particularities of space, place and the specter of surveillance to further our understanding of the broader historical and literary context in which these expatriates lived and from which the Paris Review emerged.

Distributed dystopia: Surveillance and visibility in Dave Eggers' The Circle

Session: **PARALLEL SESSION 2** – **Fiction I**

Date and time: **24th April 2014. (13:00-14:30)**

Author: **David Lyon**

In this novel about technology-and-society, a world dominated by social media is depicted as a place where privacy is deconstructed and (almost) disappears. Total transparency is the aim of the

glass-encased headquarters of the Silicon Valley Circle Corporation. The experiences of Mae Holland, their newest employee, lead us through the book. Her growing enthusiasm for being perpetually present, constantly on display and her rationalizing of each surveillance practice as necessary and beneficial is slowed only by passing qualms and suppressed unease. This paper examines the novel in three main ways: the rise of social surveillance and its merging with state, corporate and workplace surveillance; the ambiguities and contradictions of visibility in everyday life; and the coded construction of the novel itself as a vehicle for dystopian critique. The paper is framed by surveillance studies and cultural sociology in the context of debates over utopian and dystopian literature and their role in social analysis and political challenge.

From Maddam to Elysium: Projections of Surveillance in Ecological Disasters

Session: **PARALLEL SESSION 2** – **Fiction I**

Date and time: **24th April 2014. (13:00-14:30)**

Author: **Peter Marks**

The Age of the Anthropocene, a term recently adopted by environmental scholars, acknowledges that humans have exploited and reworked the planet to such an extent that they exert a determining influence on Earth's future. Surveillance has long been central to the monitoring of spaces and places, and to the ways in which boundaries between spaces are defined and maintained. How might monitoring occur in the dire environmental futures that potentially await us? This paper critically investigates the ways in which novels and films including Margaret Atwood's Maddaddam trilogy and Neil Blomkamp's recent film Elysium represent and evaluate surveillance processes in devastated environments. How would habitable and uninhabitable spaces be designated and kept separate? By whom, and for what purpose? How might identity and identification be reconfigured in times of ecological crisis, either enabling or prohibiting access to safe environments? How crucial might surveillance be to organizing a world in ecological meltdown, and how might surveillance develop to cope with these novel circumstances?

Transparent Fictions: The Changing Mise-en-Scène of (Government and) Surveillance

Session: **PARALLEL SESSION 3** – **Fiction II**

Date and time: **24th April 2014. (14:45-16:15)**

Author: **L Muir**

With the introduction and widespread use of digital monitoring technologies, contemporary understandings of surveillance are undergoing a radical re-thinking. From the previously dominant Foucauldian paradigm of discipline with surveillance carried out in (apparently) clearly-identifiable institutional contexts suggesting stability, solidity and slowness, to the ambiguous multiplicities of current surveillance practices characteristic of Gilles Deleuze's control society paradigm, a vocabulary emerges in which 'network', 'database', 'information', 'real-time', '(in)visibility', 'de/reterritorialisation', 'de/recoding', 'coercion', 'seduction' and 'flows' saturates discussions of monitoring. As a result of the fluidity and plurality of current surveillance strategies, governments have turned to a rhetoric of transparency to navigate the increasing opaqueness of a society in which monitoring is increasingly carried out in asymmetrical networks that elude easy definition.

Working within the framework of a hypothesised shift between Michel Foucault's model of discipline and Gilles Deleuze's paradigm of the control society, this paper considers the cinematic articulation of such surveillance practices. The recent release of Sam Mendes's Skyfall (2012) echoes the control logic of digital networks which focus on speed and 'invisible' modes of surveillance as the British government must counter a former 'insider' turned cyber terrorist working beyond previous institutional modes of monitoring. In contrast, Tomas Alfredson's 2011 Tinker, Tailor, Soldier, Spy emphasises the significance of materiality and slowness which is in keeping with a disciplinary framework. This potential shift in surveillance practices, often related to digital technologies, opens up complex questions for the cinematic medium in which a renewed interest in mise-en-scène becomes crucial in negotiating questions of representation. To what extent, therefore, might slowness and solidity within the visual image open up a possible space of resistance within surveillance societies which are increasingly asymmetrically networked and invisible in nature, and what can the study of film contribute to such discussions?

Mirage: surveillance in science fiction literature since 9/11

Session: **PARALLEL SESSION 3** – **Fiction II**

Date and time: **24th April 2014. (14:45-16:15)**

Author: **David Murakami Wood**

This paper presents some of the findings of an ongoing project analyzing the way in which surveillance and security have been presented in science fiction (SF) literature since 9/11, in order both to determine the impact of terrorism and the war on terror on this field and to investigate what science fiction has to say about surveillance and security. The first stage of the project systematically sampled the best SF novels published between 2002 and 2011 through the nominations for the major SF awards, ending up with a long-list of 352 novels, and coded these based by overall themem based on descriptions and reviews. The novels were then reduced to a shorter list of 87 that either won at least one award or were multiply nominated. These are being read entirely and references to security and surveillance issues noted, categorized and coded. The findings so far are that while particular examples have directly engaged with the war on terror, science fiction in generally has often only obliquely dealt with the issues and has in fact been characterized social and genre nostalgia, alternative histories and cautious or outright utopianism. However these turns are not merely reactionary, backward-looking or purely idealistic but reveal various degrees of engagement with alternative political and social possibilities that in many cases constitute implicit critiques of the contemporary security situation. In addition, these findings can be challenged, firstly because the work remains in progress, secondly because a number of SF novels published since 2011 are showing far greater overt engagement with the war on terror, and thirdly, because there are a number of very effective SF novels that deal overtly with security and surveillance issues that were simply ignored by awards committees or were relatively unpopular with SF fans. Some of these are also considered.

Metamorphosis of surveillance: from 1984 to Neuromancer

Session: **PARALLEL SESSION 3** – **Fiction II**

Date and time: **24th April 2014. (14:45-16:15)**

Author: **Nelson Arteaga-Botello**

This paper explores how literary twentieth century science fiction texts deal with the subject of surveillance. Through them, configurations of power, domination and resistance are constructed and expressed. The intention is to realize the weight and meaning given to surveillance in these narratives, as well as examining how actors negotiate, resist, and use it in order to establish some

autonomy from the powers that unfold. The literary treatment of surveillance is an imagined and idealized projection of social relations, and allows the establishment of a set of representations of actors and social events currently in progress. It is considered that literary narratives are symbolic forms that weave binary codes that reflect the possible models of social freedom and autonomy against authoritarian relationships. They are aesthetic projections and identifications, such as ongoing vital dimensions in the formation of public opinion. In this way it creates a framework where authoritarian dynamics are distinguished which are relevant to the modelling of democratic societies. The texts are classified from three kinds of societies that can be imagined: totalitarian, control and heterotopic. The stories discussed in this paper draw a repertoire of dichotomous categories that reveal social dynamics and characters in typical situations that question or idealize a series of values, such as power, domination, freedom and individuality. The intention is to realize the weight and sense that is given to surveillance in these narratives, as well as examining how actors negotiate, resist, and use it in order to establish some autonomy from the powers that unfold.

Theory

Concepts of "data": residue, resource, property

Session: PARALLEL SESSION 4 – Theory I

Date and time: **25th April 2014. (09:15-10:45)**

Author: **Dietmar Kammerer**

The paper will adress the different concepts of "data"in contemporary usage. As Rosenbaum has shown, „data "historically designated that which was given prior to an argument and thus could not be questioned (e.g. mathematical axioms). „Data "were considered to be outside the realm of the empirical. It was only with the rise of modern sciences during the 18th century, that „data" became the results of empirical research, the paradigm of what one seeks through experiment and observation. Today, in the context of surveillance and information technology, "data"is used in a variety of semantic fields. Among many more possible context, three usages of "data"will be examined more closely: In a first sense, „data" are described as the „traces" we necessarily leave when using modern media of digital communication. In this perspective, "data"are material residues, something that is left behind and that is the sign of an absence. A second context is provided by the term „data mining": Here, "data"becomes the raw material out of which a finished product or a result must be extracted. A third context is given with the rhetorical figure of the 'data double' or 'data shadow'. Here, "data"are the property of individuals in a twofold sense: that, which legally belongs to an individual (data as 'possession') and the characteristics or features that constitute an individual. The paper seeks to delineate these and more uses of the concept of "data"within surveillance discourse. The paper is a contribution to the section „theory of surveillance".

Feminist Surveillance Studies

Session: PARALLEL SESSION 4 – Theory I

Date and time: **25th April 2014. (09:15-10:45)**

Authors: **Rachel Dubrofsky and Shoshana Magnet**

This presentation provides an overview of a co-edited (Shoshana Magnet) collection of original essays entitled "Feminist Surveillance Studies" (under contract with Duke University Press), with a focus on the Introduction written with Magnet.

It is urgent that we develop critical feminist scholarship on surveillance. This work draws on feminist

theories of intersectionality to illuminate what constitutes surveillance, who is scrutinized, why, and at what cost. We contend it is necessary to look at what is at stake in current surveillance practices in terms of issues of equality and oppression, issues at the core of feminist praxis.

Undergirding the work are the questions: how might we think about the ways in which we have been asking questions about surveillance and gender across a range of disciplines? In what ways have we already been asking questions about surveillance and gender across disciplines and across time prior to 9/11 and David Lyon's work? How might surveillance put different bodies at risk/on display with particular contingencies? What constitutes surveillance? Who is scrutinized under surveillance, why, and at what cost? How are surveillance practices gendered, racialized, classed and sexualized? What are the implications for disenfranchised bodies?

Our primary interest is to think about the implications of examining concerns related to surveillance specifically as feminist issues using a feminist praxis. From cyber stalking to the policing of trans folks to the surveillance of women living in poverty, it is clear that new forms of inequalities abound. We must move beyond a simple documentation of how surveillance is occurring to develop a critical feminist perspective. Feminist scholarship provides a rich set of theoretical tools to theorize inequality, which, if focused on issues of surveillance, can bring to light the ways in which surveillance is tied to systemic forms of discrimination.

(Un)seeing Dead Bodies: An Exploration of the Visual and/in "Terrorist" Deaths

Session: **PARALLEL SESSION 4** – **Theory I**

Date and time: **25th April 2014. (09:15-10:45)**

Author: **Priya Dixit**

In scholarship on terrorism, concerns of visibility are often ignored. This is problematic because the label "terrorism" and the language of the "war on terror" make certain actors and spaces ("terrorists", those who support them, those who counter them, those who respond to them in other ways) visible and other actors and spaces (other non- "terrorist" issues, sites where "terrorists" or those deemed as aiding "terrorist" are kept, texts and documents labelled "national security", etc) invisible. Even if events and actions are irreducible to words, they have to be represented, embodied and performed. Here, I would like to draw on insights from postcolonial and black feminist thought to theorize the representations, embodiment and performances of "terrorist deaths"—that of Osama bin Laden, Anwar al-Awlaki and the many others whose names the public is never told. I am especially interested in studying these deaths (and the practices of killing) in

terms of what the representations and “viewings” (or not viewing) of such deaths means to our understanding of visuality and security.
There is a duality to visuality—potential “terrorists” are made visible by technological surveillance but their deaths are often invisible and take place out of “our” sights. In many ways, these contemporary practices of surveillance parallel colonial responses to resistance fighters and historical surveillance of women and minorities. By drawing out these connections in the context of “terrorist” deaths, and discussing who has “the right to look” (as Nicholas Mirzoeff has called it), a counterhistory of visuality and security may be outlined. Overall, this paper’s focus remains on practices to decolonize the (surveillance) gaze as I study “terrorist” deaths as events where the surveillant gaze is, perhaps, resisted and reconfigured.

Neoliberal Forms of Surveillance: A Strategic Dissection and Re- Articulation

Session: **PARALLEL SESSION 5** – **Theory II**

Date and time: **25th April 2014. (11:00-12:30)**

Author: **William Lockrey**

In times consumed by the prospects of ‘big data’, widespread and ubiquitous proliferation of preventative, or ‘speculative’, surveillant technologies have dominated the security landscape. There have been many explanations as to why these algorithmic technologies continually spread, often in a zero-sum game where security and privacy are continually traded for one another for example. And while many scholars do indeed point to Neoliberalism as a guiding principle, it is widely assumed as understood or a homogenous concept; While failing to discuss, in-depth, the particular nuances that appear to play a substantial part in creating and shaping lucrative, entrepreneurial markets that thrive in times of insecurity. This article seeks to illustrate how the commodification of ‘fear’ and ‘uncertainty’ has resulted in active market-creation in a multi-scalar fashion through a myriad of heterogeneous means. By analyzing public perceptions of ‘security’ as measured by the Globalization of Personal Data (GPD)* dataset under the theoretical lens of Neoliberalization we can begin to understand the growth of surveillance as the result of meticulously created entrepreneurial environments that spread through avenues that are wholly ‘Neoliberal’ in nature such as: fast policy, the authenticity of supranational bodies, and transnational rule regimes.
*The GPD dataset was created by the Surveillance Studies Centre (SSC) at Queen’s University. Details of the GPD can be found at: http://www.sscqueens.org/projects/gpd

From Lifestyles to Locations: Theorizing Surveillance in Location Based Services

Session: **PARALLEL SESSION 5** – **Theory II**

Date and time: **25th April 2014. (11:00-12:30)**

Author: **Harrison Smith**

Surveillance, as an institutional gaze for normalizing bodies and subjects, is increasingly moving towards mobile and ubiquitous computing environments. One such example is Location Based Services (LBS), GPS enabled smartphone applications which ubiquitously track location in the delivery of particular information or services. LBS can be theorized as a form of consumer surveillance which complicates but also compliments pre-existing forms of knowledge production and consumer analytics, particularly geodemographics.

This paper will explore LBS as a form of geodemographic knowledge production and lifestyle market segmentation based around the analysis of mobility patterns. It will first present an overview of key academic research, and examine the emerging questions relevant for surveillance studies, particularly as it concerns the negotiation between institutional orderings of self and vernacular epistemologies of everyday life. The politics of how institutional developers understand LBS will be the primary focus here; the paper will present an analysis of industry literature and white paper research produced by relevant industry organizations in order to identify the underlying discourses and beliefs of LBS developers.

Exploring the "seduced" surveillant subject

Session: **PARALLEL SESSION 5** – **Theory II**

Date and time: **25th April 2014. (11:00-12:30)**

Authors: **Pinelopi Troullinou**

In western societies, the dependence on Information and Communication technologies (ICTs) is rapidly increasing. The use of digital technologies in everyday life is widespread and individuals seem to use their digital gadgets everywhere "from the dining table to the bathroom and bedroom" (Ofcom, 2011) as they promise to offer them communication, entertainment and convenience "all in one". At the same time though digital devices can be (ab)used as means of facilitating surveillance as the data provided online can be readily available to be monitored, tracked, processed and manipulated (Andrejevic, 2012; Lyon, 2001) for different reasons than the ones originally intended

to. However, focusing on the smartphones as a case study, based on a recent Ofcom research (2013) that reveals young people in the UK to be addicted to them, the present paper argues that their usage is considered as part of social and cultural practice in accordance to consumption and thus "disregards concerns about data protection and consumer surveillance" (Zurawski, 2011: 518). Smart phones promise a whole new experience to their users and therefore users do not fully comprehend how their data can be exploited and used by both the state and the market in the late capitalism context. Thus, the present paper drawing upon mainly surveillance, organizational and marketing literature argues that smartphone devices are part of "seductive surveillance" according to which the surveillant subject is "seduced" by the dominant marketing ideology and discourses surrounding the devices, into performing work in his/her own surveillance providing willingly more and more data. Academics underline the need then to explore subjectivity, towards which the present paper aims to contribute, as it has not received yet extended attention in surveillance studies even though crucial concerns of surveillance practice are inevitably related to it (Harper et al., 2013; 187). It becomes urgent to explore the subjective experience of surveillance to understand whether the subject relates the everyday practices of smartphone usage to surveillance methods, and whether they feel exposed to surveillance (Ball, 2009; Harper et al., 2012) in order to shed light on possibilities of resistance.

How was it for you?:Carnivalesque in reflections on a Multi-Disciplinary Surveillance and Organization Research Project

Session: **PARALLEL SESSION 6** – **Theory III**

Date and time: **25th April 2014. (13:30-15:00)**

Authors: **Keith Spiller, Kirstie Ball, Liz Daniel, Sally Dibb, Maureen Meadows and Ana Canhoto**

This paper considers the reflections of 6 researchers who worked together on a 3 year research project. The researchers came to the project from a range of disciplinary traditions and with, what could be viewed as, different perspectives on how to conduct research in surveillance and organization. As far as we know no previous work has involved an organisational theorist, a marketer, a management strategist, a human geographer, an information system expert and an surveillance scholar. The paper asks, what happens when researcher's theoretical assumptions are challenged and/or broadened by colleagues? For some time now the advantages of multi-disciplinary approaches have been encouraged by funding bodies. We argue for clarity and attention to be paid to multi-disciplinary approaches and we discuss how we have understood the

collaborative process of researching, thinking and writing. Throughout our project work we have conveyed and elicited knowledges to each other that were, at times, new to us – equally, not all of these new knowledges worked but this too is part of the collaborative process. Consequently we begin the paper with vignettes written by us, the researchers, about our theoretical journeys during the research project. In developing our argument we consider the retrospective and reflexive qualities expressed in our vignettes. We begin by examining the collaborative process and consider the 'new knowledges' which resulted from our collaborative theorizing. These knowledges we contend generated important findings and important methodological contributions to how surveillance and organization is researched.

The affective dimension of surveillance

Session: **PARALLEL SESSION 6** – **Theory III**

Date and time: **25th April 2014. (13:30-15:00)**

Author: **Richard Jones**

This paper aims to outline the contours of possible study of the emotional dimensions to surveillance. Whereas there exists a substantial and convincing body of research on aspects such as the practical operation, instrumental aims and wider social roles of surveillance, another possible line of enquiry is to explore the emotional reactions experienced by those involved in the production and consumption of surveillance media. Surveillance typically involves either the surveillance of communications media, and/or the generation of surveillance media recording and documenting people's activities. Drawing from research in media studies and cognate areas, and focusing in particular on studies of the reception and interpretation of media, this paper argues that the emotional experiences attendant in the production and consumption of surveillance media, as well as the emotional experiences involved in being the (potential) target of surveillance, are not only important but sometimes marginalised qualities of surveillance, but may also be revealing as to what is most problematic about surveillance. As such, it is further argued that the affective dimension of surveillance is intimately related both to individual sensibilities about privacy and to political concerns surrounding surveillance's use. Through reference to certain illustrative examples, the paper develops a simple theoretical framework to help guide research in this area. The paper concludes by exploring the implications flowing from this analysis, both for academic research and political action.

Surveillance of cultures, cultures of surveillance

Session: **PARALLEL SESSION 6** – **Theory III**

Date and time: **25th April 2014. (13:30-15:00)**

Author: **Antonella Galetta**

Surveillance is considered as one of the key dimensions of the modern world and actually it is so. It was not the PRISM scandal that made us aware of this state of affairs. Rather, PRISM has been just the confirmation of an unspeakable truth which had raised the concerns of many. The massive deployment and use of surveillance technologies in contemporary societies tells us that it is not necessary to wait for the next 'surveillance wave' to claim that we live in a surveillance culture. Although this statement would hardly find dissenting opinions within the surveillance literature, it is still not clear to what extent the different societal actors contribute to build that culture. Similarly, it is not apparent to what extent they should be considered accountable for the burden of the surveillance culture we are living in. Given the incapability of law to keep pace with technology developments for example, it is often argued that courts should take the responsibility for deciding about the legitimacy of certain surveillance measures. However, this is often hardly feasible from a legal point of view and barely acceptable from an ethical perspective.

This paper will investigate how contemporary societies are permeated by surveillance and how different societal actors are shaping our surveillance cultures. In particular, it will focus on the role of citizens as passive but also active actors of the 'surveillance game'. The main thesis of this paper is that, although governmental authorities are key promoters of the surveillance culture, that very culture is also the result of individual choices taken by citizens in their everyday life. Thus, although citizens live in surveillance cultures nowadays, their choices contribute to shape that culture.

Opening the closed. A merciful and erotic interpretation of surveillance, vision and gaze

Session: **PARALLEL SESSION 7** – **Theory IV**

Date and time: **25th April 2014. (15:15-16:45)**

Authors: **Susanne Wigorts Yngvesson**

Within the discipline of Christian theology there are several examples of theology as surveillance, for example pastoral care, confession and the moral system as a producer of guilt. The awareness of sin can be interpreted as a form of self-surveillance and a social control system (Luther;

Foucault). This paper will include a brief discussion about Christian theology and an interpretation of it as a surveillance system. But the main focus will be an analysis of a Christian theology as an alternative to an inner logic of surveillance. For example, the Eye of God can be experienced as both an unpleasant power and as a liberating power. When St Augustin speaks about the vision of God in his Confessions, it is a vision that reveals perspectives of the world he cannot see on his own. He needs God to open his vision. When Luther argues for his view on vocation it is described as a system of surveillance and confirmation. This thought is quite common through the biblical texts and I will interpret some of them to develop a critique towards surveillance as an inner logic of utilitarianism and symmetry. It is a gaze of mercy, and it is recognized by an erotic power of love between God and human or between humans. It is a vision that "sees the in-visible in the visible" (Merleau-Ponty) and starts in an open attitude of trust and expectation. The vision of bodies is in this perspective not a categorization, but an open gaze that looks "behind" or "inside" the body, as when people in the Bible meet Jesus and experience he can see into their hearts. (Augustine; Nordlander; Kearney)

Integrating subjects: Linking surveillance experiences to social patterns using Ethno-Epistemic Assemblages

Session: **PARALLEL SESSION 7** – **Theory IV**

Date and time: **25th April 2014. (15:15-16:45)**

Author: **Ashlin Lee**

Surveillance can be experienced in a variety of ways, but how these experiences might be linked to broader social patterns is currently underdeveloped. There is a growing body of research exploring the surveillance subject and how individuals may (dis)engage with surveillance practices. This includes (but is not limited to) surveillance as a bargaining process (Pallitto 2013), counter surveillance activities such as sousveillance (Mann, Nolan and Wellman 2003), and surveillance as a process of exposing subjects (Ball 2009). But while shedding light on the experiences of surveillance subjects, how these experiences might be placed in relation to broader social and surveillance structures is not always automatically evident. This paper presents an initial engagement with this topic, and suggests that a possible angle for linking surveillance subjects to broader social patterns may be achieved through concepts from science and technology studies, specifically Irwin and Michael's (2003) concept of the ethno-epistemic assemblage (EEA). The EEA is a theoretical heuristic originally envisioned to help understand the blurred relationships between science and society, emphasising the heterogeneous composition and relationship of

technoscience and society. The EEA specifically links an individual's contexts (ethnos), and the forms of knowledge relevant to their contexts (episteme), into assemblages, highlighting the interwoven, dynamic, and fluid nature of ethno-epistemes against and in conjunction with other EEAs, and other social narratives. A brief exploration of the marginal positioning of surveillance subjectivities is presented, followed by a detailed description of the EEA, and how it may contribute to structuring and placing the complexities of surveillance subjects in society.

Data-Other and Asymmetry

Session: **PARALLEL SESSION 7** – **Theory IV**

Date and time: **25th April 2014. (15:15-16:45)**

Author: **Daniel Slavicek**

David Lyon, but also other scholars such as Lucas Introna, pointed out importance of Emmanuel Levinas´s work for multidisciplinary field of surveillance studies, especially when discussing ethics of surveillance. In my paper I attempt to discover meaning of asymmetry in Levinas´s work and I would like to compare this kind of asymmetry with asymmetry used mostly in the discourse of surveillance studies. Secondly, I would like to present my notion of the data-Other which is derived from Levinas´s work.

Levinas´s key theme of encountering with the Other could be found already in his early works after the second world war, but comprehensively is presented in his first masterpiece Totality and Infinity, written in 1961. Here he calls into question whole philosophical tradition that poses the Same (subject, self, I) as a source of knowledge and freedom. For Levinas, it is the Other (Infinity) who problematizes the subject and that is why ethics precedes ontology, because the Other gives meaning to the Same. Other is manifested in his face, which speaks the first words of ethics "Do not kill me". Asymmetry could be found exactly here between the Same and the Other. But it is the Other, who is the Master, whose face is a sign of Infinity. When we speak about asymmetry of surveillance, we mostly understand the asymmetry between those who watch and those who are being watched. We think of power of the first and powerlessness of latter. But for Levinas, it is the Other, who is above me, and to whom I am responsible that much, that I become hostage to the Other as presented in Levinas´s second masterpiece Otherwise than being. Digitally mediated world in which we live in these days raises many ethical questions. Surveillance and control are one of the most important. Different concepts of surveillance studies describe, how are our identities dispersed in the virtual worlds and we lose control over them. Concepts such as

dividuum (Deleuze), data-double (Haggerty and Ericson), data-image (Poster), digital persona (Clarke) describe similarly this phenomenon. But in the context of Levinas´s work, we can change the optics and ask, whether the virtual worlds do not require its own ethics based on something which I suggest to call the data-Other. Maybe we should start to think about the billions of personal details and images as about traces of the Other. Richard A. Cohen mentions, that e-mail or letter could be understood as the face of the Other. I disagree with that idea, but to understand data-Other as ethically undertaking may open new meaning to the ethics in the virtual worlds.

The Art of Governing in an Age of Revelation: On the Biopolitics of Biovisuality

Session: **PARALLEL SESSION 8** – **Theory V**

Date and time: **25th April 2014. (17:00-18:30)**

Authors: **Gavin John Douglas Smith**

This paper examines the transforming value, resolution and vitalism of the social body as it is increasingly informationalized, visualized and anatomized by multivalent systems of exposure. Multiplex biopolitical interests influence and incite these practices: wills to discern and direct consumption habits; ambitions to inscribe structured meanings upon somatic territories; and desires to better identify, verify and assess corporal components. An emerging confluence of biovisual imperatives, practices and flows are placing unique demands on embodied subjects, specifically concerning (a) the control, ownership and arrangement of personal information deriving from bodily interference, and (b) the types of performative exertions and authentication protocols that are now routinely requested and indeed expected at various visualization contact points (McGrath 2004; Andrejevic 2012). In an age of somatic magnification and scrutiny (Monahan and Wall 2007), where fleshy topographies are considered as stable sites for truth adjudication and as volatile sites for correctional modulation, the sociological imagination can help excavate several resonances attendant on the proliferation of biocapturing mechanisms and on concomitant conditions of biovisuality. As I will argue, repetitive bioexposure, as both involuntary dictate and volitional act, generates de-contextualized knowledge streams, the channeling of which can assist experts in sharpening their diagnostic definitions and honing their prognostic interventions. But it also produces curious subjectivation effects at the phenomenological level. Subjects become accustomed to exteriorizing interior confidences and revealing subjective states in the form of informatic particles (Foucault 1988). In this process, personal intimacies become public property, a situation inducing social harms and igniting insurgent possibilities. A critical consideration of these

issues, specifically their interconnectedness and biopolitical significance, occurs in the paper as it focuses analytical attention on the types of subjectivity being fashioned from bodily transmissions and transitions.

Reclaiming the Look- Red Road as Feminist Surveillance

Session: **PARALLEL SESSION 8** – **Theory V**

Date and time: **25th April 2014. (17:00-18:30)**

Author: **Jonathan Naveh**

Traditionally in the cinema surveillance is used as a means to confront the anxiety of being watched (or listened to) in social and to a lesser extent, private, spaces. The roles of women in films like The Conversation, Klute, and Enemy of the State are as temptresses, victims, and peripherally relevant characters. In a genre working through notions of scopophilia and looking as social structures, there seems no place for women to contain a mastery of their own look. The Hollywood films equate looking with patriarchal structures, to a degree enforcing Laura Mulvey's contentions over the ways in which Classical Hollywood uses and gazes at women. With Red Road (2006) Andrea Arnold presents a film that features a female protagonist in the position of a surveillance operator. Arnold offers this protagonist a distinct control over her look given her occupation, but also a sense of agency that seems absent from the patriarchal regimes of other surveillance related films. The fact that Arnold as a director is also a female (within a subgenre of male-directed and male-centered-narratives) elevates the product to a level of feminist counter-cinema, one whose aim is to propose the female look as salient to surveillance narrative and the enforcement of personal and social spaces.

Post-Communism: What does it mean in a surveillance studies perspective?

Session: **PARALLEL SESSION 8** – **Theory V**

Date and time: **25th April 2014. (17:00-18:30)**

Authors: **Ola Svenonius, Fredrika Björklund and Pawel Waszkiewicz**

It is well known that surveillance was a key aspect of daily life in the communist regimes in Central and Eastern Europe. Despite vast differences between societies, techniques such as infiltration and wiretapping were endemic. The 'discourse of real socialism' that legitimated such practices favoured an obedient, introvert and passive subject, whereas the capitalist-democratic system of today (in theory) demands the opposite (Alexander and Smith 1993, as quoted in Sztompka

2001:22). We are interested in how these opposing discourses play out in attitudes on surveillance in today's post-communist societies. Some hypotheses exist in this area. Piotr Sztompka, for example, has discussed the perseverance of the old communist 'habitus' in these countries: personality traits in the general population that bears signature of the communist surveillance (op cit). While interesting, this kind of reasoning threatens to over-emphasise the role of the past in present attitudes towards surveillance.

This discussion is the point of departure for outlining the concept of an international survey in Estonia, Poland and Ukraine that will be carried out during the first half of 2014. Using the theoretical debate on post-communism in the social sciences, and existing survey research in the surveillance studies as starting points, we present an argument about how surveillance can be studied in post-communist contexts that focuses on experiences of everyday versus secret surveillance, trust, and social equality.

Privacy

The economics of surveillance and privacy

Session: **PARALLEL SESSION 5** – **Privacy I**

Date and time: **25th April 2014. (11:00-12:30)**

Authors: **Gemma Galdon Clavell and Álvar Garola**

In recent years academics and public servants have given increasing thought as to how to assess the merits and drawbacks of laws, policies and investments centred on surveillance. Classic cost-benefit analysis has centred on the harm caused by certain crimes, the perceived utility of surveillance technology and the assumption that the public are somehow willing to 'trade' rights such as privacy and conveniences such as free movement for more security. 'Privacy impact assessments' have emerged as a central means by which policy-makers can assess the extent to which such a trade-off is actually necessary, while the principle of 'privacy-by-design' is supposed to minimise the impact on individual rights. Ethical reviews have characterised proposals for public investment into research and development of new surveillance technologies. Technology assessment and post facto reviews of effectiveness are also shaping policy decisions, as are relevant rulings by national and federal courts on the limits of existing surveillance systems. However, a consolidated model to assess the economics of surveillance taking into account social and legal externalities, as well as issues of trust and acceptability has not yet emerged. The work that will be presented aims to shape nascent discourses on the economics of surveillance and security policy impact assessment. By drawing on tools from environmental impact analysis, public policy and surveillance studies, the proposed methodology will provide decision-makers with practical tools to make better and more accountable decisions while helping the security industry better understand the long-term cost of hidden social and legal externalities of surveillance technologies.

From password to pepper spray: Associations in the context of surveillance

Session: **PARALLEL SESSION 5** – **Privacy I**

Date and time: **25th April 2014. (11:00-12:30)**

Authors: **Sandra Appleby-Arnold, Noellie Brockdorff and Daniele Mezzana**

Whilst those institutions or individuals who implement technological surveillance measures often claim that these aim to increase either national security or citizens' personal safety, it has become

increasingly accepted that such security will, inevitably, generate forms of insecurity as by-products. Fuelled by economic and political instabilities on a global scale, risks and uncertainty have supposedly become part of our everyday lives. But do we really live in such multi-leveled cultures of fear? Within SMART, a collaborative project co-funded by the European Union, research was conducted to explore citizens' attitudes towards surveillance and privacy. As part of this study focus group discussions with a total of 320 participants in 14 European countries were carried out. At the beginning of each discussion, before the topic of surveillance was introduced, participants were asked to freely associate with terms such as privacy, national security, and personal safety. This unstructured and indirect soliciting of response encouraged respondents to project their underlying motivations, feelings or beliefs. Combining the word association study with content analysis and following a multidisciplinary approach, the qualitative results reveal a more nuanced picture relating to concepts of surveillance and protection. Neither privacy nor personal safety were predominantly associated with absence, loss or violation, but rather associations appeared to be influenced by local incidents, specifically related to dataveillance, or to perceptions and constructions of privacy itself. Associations with national security were, partially, linked to local political histories, but self-responsibility and self-defence appeared to play the more important role. These findings suggest that citizens' attitudes to surveillance and personal safety may differ from those found in other studies based on direct questions. They shift the focus to more complex conceptualisations of protection where asymmetry may be both defective and productive.

IPO 2.O: The Panopticon Goes Public

Session: **PARALLEL SESSION 5** – **Privacy I**

Date and time: **25th April 2014. (11:00-12:30)**

Author: **Greg Elmer**

To suggest that privacy is dead is not to revel in or encourage its demise, nor even to claim that it is not a desirable outcome, right, or valued policy. Rather, what this paper suggests is that in certain circumstances (increasingly on social media platforms) the privacy of users now stands in direct opposition to the stated goals and logic of the technology in question. One need not give up certain goals of privacy to recognize that business models of online companies like Facebook and Google are now entirely predicated upon the act of going public—there would be no Google search engine or Facebook social networking platform without the content, information, and demographic profiles uploaded, revised, updated, and shared by billions of users worldwide.

This paper then offers some initial thoughts on a theory of publicity, of going public in the social media age. If social media platforms are governed by ubiquitous surveillance and continuous uploading and sharing of personal information, opinions, habits, and routines, then privacy would seem only to be a hindrance to these processes. To ignore such clear mission statements, coupled with repetitive attempts to undermine, display, and obfuscate so-called privacy settings, would seem disingenuous at best, and willfully blind at worst. These online platforms profit from publicity and suffer from stringent privacy protocols—their whole raison d'être is to learn as much as possible about users in order to aggregate and then sell such profiled and clustered information to advertisers and marketers. Can we really conclude that such businesses violate users' privacy when their platforms are in the first and last instance wired for ubiquitous publicity? Or more to the point, do privacy-based perspectives provide an adequate framework for understanding users' relationships with social media platforms and their parent companies?

Profiling: risks, potentials and room for action

Session: **PARALLEL SESSION 5** – **Privacy I**

Date and time: **25th April 2014. (11:00-12:30)**

Authors: **Daniel Guagnin, Valeria Ferraris and Niklas Creemers**

In the bigger framework of "Surveillance Ambiguities & Assymetries" this paper focuses on control through technology, more specifically machine profiling. It will deliver a definition of profiling and explore infringements of fundamental rights and moral values emerging from current profiling techniques.

This paper will firstly examine the technological evolution of profiling to outline a definition of nowadays machine profiling practices. This techno-historical approach allows to elaborate the specific issues surrounding dataveillance today including some of its subtle features (i.e. the fact that most of the data are neither personal nor sensitive and are user-generated or generated for administrative purpose) and its ubiquitous nature.

In its second stage, the paper will tackle the risks that profiling can entail with regards to fundamental values (such as democracy, rule of law, autonomy and self-determination) and rights (such as right to privacy and data protection and right to non-discrimination). Power asymmetries established and deepend by the growing abilities of processing and analysing big data is one aspect which will be taken into account.

In a third step the paper will display technological trends and social and political potentials and risks

linked to them. Main aspect will be the question which room for action is and will be left for citizens on the backdrop of the growing realms of application of profiling technologies.

The paper will conclude outlining blind spots in the profiling debate, included the current discussion on draft GDPR, and future research questions.

This paper is drawn from the background studies conducted for a EU-funded project named PROFILING that commenced in November 2012 (http://profiling-project.eu).

The Sale of 'Edited' Electoral Registers in Scotland: Implications for Citizenship, Privacy and Data Protection

Session: **PARALLEL SESSION 6** – **Privacy II**

Date and time: **25th April 2014. (13:30-15:00)**

Authors: **Charles Leleux and C.William R. Webster**

The proposed paper provides an assessment of the growing phenomenon in Scotland and the United Kingdom of the sale of 'edited' electoral registers to third parties, and reflects on the implications which this has for state and citizen relations, privacy and data protection. New legislation was introduced in Scotland in 2002 (Representation of the People (Scotland) (Amendment) Regulations 2002) which requires Electoral Registration Officers to compile a separate 'edited' electoral register for those electors who do not wish their names included in a register which could then be sold to third parties. Comparison is made with the role of data aggregators in the United States, which according to Bennett (2013), are selling profiling information to political parties farmed from electoral registers for the targeting and canvassing of electors. Drawing upon the results of a survey of Electoral Registration Officers in Scotland, information will be provided on the sales of 'edited' registers since 2002 including approximate revenues and importantly the categories of organisations involved. Calls for the sale of 'edited' registers to be abolished have been raised by various actors, including the UK Information Commissioner, The Electoral Commission, and the Political and Constitutional Reform Select Committee of the UK Parliament. Contrastingly, the UK Parliament and Constitution Centre (2012) advised that support for the retention of the practice has been voiced by marketing companies, credit reference agencies and debt collection companies. Recently, a report by Big Brother Watch (September, 2013), raised concerns about the possible lack of awareness amongst electors that this practice is occurring, and that the selling of the 'edited' registers is possibly deterring them from voting. The practice of selling 'edited' electoral registers strikes at the heart of democracy in that the state has potentially eroded trust in citizen-state relations by allowing citizens' personal

information to be sold to third parties in an unrestricted and apparently haphazard manner.

Incautious Porn, an anthropological experiment in blackmail and the perception of private/public space online

Session: **PARALLEL SESSION 6** – **Privacy II**

Date and time: **25th April 2014. (13:30-15:00)**

Authors: **Salvatore Iaconesi and Oriana Persico**

We have radically changed our perception of what is public and what is private. While using social networks, search engines and websites determining who has access to our information, our personal details, our habits and preferences is often complex or not easily accessible.

Each person's information is sold hundreds of times each day, while surfing websites and social media sites, with information passing from one provider to the other in ways that are subtle and non-transparent: data collected on one site may be used on other sited to sell us advertisements or to investigate on our lives.

On top of that, most people tend to interpret social media sites as new forms of public spaces, and it is fundamental for service providers' strategies that this perception is maintained, to promote our full disclosure, allowing them to collect even more data about ourselves.

We used the project Incautious Porn to investigate on this scenario, to explore the shifting and blurring of the boundaries of what we perceive as our privacy and as our private and public spaces.

Incautious Porn uses the operations of a fake company systematically invading our privacy (even to the point of performing simulated forms of blackmail) to collect enormous amounts of information which we have used to analyze this scenario.

In Incautious Porn art acts both as a sensor on the transformation of human societies and as a tool for analyzing its effects.

The effects of the Incautious Porn project and communication campaign have been massive, bringing it to the attention of a large, global, audience and, thus, allowing the research team to benefit from a large data set.

Furthermore, the actions of the blackmailing fake-company have been led using an ethical approach: no money was taken from people, and all their personal data has been preserved, also using the initiative as a testing lab for novel privacy and security preservation techniques, and as a campaign for awareness about the transformation of people's perception of contemporary private/public spaces.

Habeas What Corpus? Privacy and the Place of the Body in Surveillance Societies

Session: **PARALLEL SESSION 6** – **Privacy II**

Date and time: **25th April 2014. (13:30-15:00)**

Author: **Charlotte Epstein**

In this article I seek to understand how technologies and practices of surveillance are changing our experiences of bodily privacy. To this end use a surveillance technology explicitly centred upon the body, biometrics, as a field for tracking the changing relationships between the body and privacy that underwrite our modern democratic polities. Adopting a broader genealogical perspective, however, I begin by retracing the role of the body in the constitution of the modern, liberal political subject. I consider successively two quite different understandings of the subject, the Foucauldian political subject as theorised by Michel Foucault, followed by the subject of psychoanalysis in the wake of Jacques Lacan. My genealogy of the modern political subject begins with the habeas corpus, and observes a classically Foucauldian periodization, the historical succession of a 'regime of sovereignty' with a 'regime of governmentality' within which our surveillance societies are currently taking shape. In the final part of the article I then reverse the direction of the gaze, and consider the subject looking back or rather into the mirror. I consider the place of the body in the constitution of the psychic subject in Lacan's mirror stage, and conclude to the importance of privacy in the development of the psychic subject. The psychoanalytic perspective, in which the gaze of power is revealed as the gaze of the Other, serves to appraise the effects upon the subject of being exposed to constant viewing. By considering these two facets of subjectivity – political and psychic – I hope to make sense of our enduring passionate attachment to privacy, notwithstanding the normalization of surveillance technologies and practices.

Political

Politics of Disappearance in Practice: Interrogating Surveillance's Ob-scene

Session: **PARALLEL SESSION 5** – **Political I**

Date and time: **25th April 2014. (11:00-12:30)**

Authors: **Rocco Bellanova, Gloria Gonzalez Fuster and Raphaël Gellert**

This contribution studies modern surveillance from the perspective of a politics of disappearance. The notion of politics of disappearance problematizes the presence and absence of disparate elements in concrete practices. It aims to illuminate typically neglected styles of association composed not only of what is visible, but also of what is left out, hidden or excluded. By doing so, it can contribute to move beyond conceptualisations of surveillance entrenched in discussions of who observes what, what is observed, and what is observable.

Two case studies illustrate this approach. First, the paper considers how recent revelations about United States (US) National Security Agency (NSA)'s surveillance programs blur the distinction between overt and covert surveillance, and grant a productive role to the concealed. Ranging from the ghostly presence of whistle-blower Edward Snowden to the seemingly un-fathomable nature of existing monitoring practices, these revelations help to exemplify the tensions between visibility and invisibility in contemporary surveillance.

Second, the paper looks into so-called resistance practices, and particularly into how activists struggle to re-activate seemingly endangered notions such as subjectivity and privacy through a saturation of nakedness. In this context, exposure is used to reclaim a right to hide, and revealing becomes a mode of contestation.

These cases allow interrogating the meaning of the ob-scene, by bringing to the fore what is deliberately left aside, deleted, banned, and questioning how it can operate.

The idea that ob-scene elements are vital to modern surveillance notably obliges to critically assess calls for 'transparency' as a response to its deployment. If surveillance practices are not only ambiguous but, in a sense, inherently translucent (never fully present, but never fully absent) perhaps emerging politics need to refine the way in which they embrace their understanding of disappearance.

Algorithmic surveillance and security: political visions and social boundaries

Session: **PARALLEL SESSION 5** – **Political I**

Date and time: **25th April 2014. (11:00-12:30)**

Author: **Jens Hälterlein**

I would like to address the role new technologies play in contemporary crime control by illustrating the development and implementation of algorithmic surveillance systems in Germany. Since this technology is not based on the psychological or criminological analysis of deviant individuals, but on the analysis of situation, space and groups classified as dangerous, it can be seen as a signature of a new rational of crime control, described by scholars as situational crime prevention, new penology or neo-liberal governmentality. In this new rational, algorithmic surveillance is seen as an efficient and effective tool for security measures. In accordance with this view both, advocates and critics of this technique draw a picture of new powers of control, that stretch from terrorism and incivilities to mass events. This vision of technology based security yet faces technological problems (how can indexical behavior be translated into software algorithms?) and the often divergent interests of prospective users (police, public transport, private enterprises). Drawing from empirical research conducted for the German FMER-funded MuViT project and the EU-funded Videosense project I want to show, that the development of algorithmic surveillance systems is on the one hand part of a new rational of crime control since it comes with a re-coding of risk and security. On the other hand its practical implications correlate with a multitude of social factors.

Surveillance as Domination? Putting the Neo-Republican 'third concept of liberty' and Surveillance Studies in Conversation

Session: **PARALLEL SESSION 5** – **Political I**

Date and time: **25th April 2014. (11:00-12:30)**

Authors: **Matthew Hoye and Jeffrey Monaghan**

Presently, the analytical language of surveillance studies is overwhelmingly that of post-structuralism. For good reason. Unlike Marxist and liberal frameworks, post-structuralism is well equipped for the study of surveillance. However, the language of post-structuralism is very specific and is not couched in a broader political language, thereby cloistering surveillance studies to a very specific audience. This is problematic because a robust critique of state surveillance—and a

general resistance to surveillance practices—requires that critiques of surveillance be hitched to a broader political language of freedom. If post-structuralism does not proffer a suitable language for a more general critique, while the languages of freedom on offer by liberal and Marxist (negative and positive liberty) are incompatible with the critique of surveillance, then the critique of surveillance will remain marginal. In the last 25 years, and quite apart from the surveillance literature, a 'third concept of liberty' has been historically excavated and analytically honed by, respectively, Quentin Skinner and Philip Pettit. In contrast to the liberal conception of freedom as 'freedom from interference', at the heart of the neo-republican conception of freedom is the claim that freedom is freedom from domination. The question then—the question that our paper will broach—is, does this third concept of liberty and its constellation of political ideas provide a political language amenable to the concerns and critiques of the surveillance literature. If so, how? By way of example, we discuss the NSA surveillance scandal and suggest how a neo-republican analysis can inform responses to these practices of state surveillance.

Exercising access rights in Spain: legal provisions vs. practice

Session: **PARALLEL SESSION 6** – **Political II**

Date and time: **25th April 2014. (13:30-15:00)**

Authors: **Liliana Arroyo Moliner and Gemma Galdon Clavell**

This paper presents the preliminary results for the Spanish case study on access rights within the framework of the EC-funded IRISS3 project.

The paper summarises the process and results of exercising the right of access in 30 sites based in Spain, in domains as broad as: health, transport/holidays, work, education, finances, leisure, communications, consumerism, and civic engagement. Within these domains, specific research sites were identified and approached.

The method used has been ethnography in two phases: one in locating the data controllers and the second sending subject access requests. The requests included questions related to personal data disclosure, the use of automatic making decision processes and data sharing with third parties. Strategies of facilitation and denial have been recorded, along with successful and unsuccessful cases.

Primary results show how compliance with the data protection law is the exception, especially in public institutions (even if the results show bad practice across the board). Often times, failure to comply with the law is also associated with more subtle denial and delay strategies aimed at

discouraging the citizen from exercising his/her rights. In the end, the picture that emerges shows a landscape of unawareness of the legal framework, disregard for data protection and vulnerability.

What do they know? Exercising subject access rights in democratic societies

Session: **PARALLEL SESSION 6** – **Political II**

Date and time: **25th April 2014. (13:30-15:00)**

Authors: **Xavier L'Hoiry and Clive Norris**

The significance and importance of the so-called ARCO (Access, Rectification, Cancellation, and Opposition) rights has grown alongside the ongoing proliferation of surveillance and data collection techniques enabled by technological advancements. Amongst the ARCO rights, one may consider 'access' as the natural 'pre-condition' for citizens to exercise the full spectrum of their rights of informational self-determination. Put simply, citizens must know what is held about them before making an informed judgement about how these data should be processed (and by whom).

With this in mind, this paper will present the results of our multi-partner FP7 project on surveillance and democracy entitled IRISS. In particular, we have focused upon the ability of citizens to exercise their democratic right of access to their personal data. Together with ten partner institutions, we conceptualised a research approach involving auto-ethnographic methods which sought to 'test' how easy or difficult it is for citizens to access their personal data. Specifically, this process was broken into two distinct phases. The first phase concerned locating data controllers and their contact details in order to actually request access to personal data. The second phase of the research was concerned with making the requests and documenting the process of accessing one's personal data from the moment a request is made to the eventual conclusion, whether this results in successfully receiving one's personal data or not. We will present the overall findings of the ten country study and consider the strategies used by those who hold our personal data to facilitate or deny us access to what they know about us and how they process it.

Swamp Island: Surveillance and White Supremacy in the Progressive Era U.S. South

Session: **PARALLEL SESSION 6** – **Political II**

Date and time: **25th April 2014. (13:30-15:00)**

Author: **Annette Louise Bickford**

U.S. empire not only produced overseas others, but also carefully monitored the Other within the nation's interior frontiers through a kind of internal colonialism, focusing on white domestic life, families, and miscegenation. Discourses of the U.S. South as an uncivilized, foreign and dangerous region—a nation within a nation—reached their peak during the Progressive Era, at the height of American imperial expansion overseas. The U.S. South held a particular fascination for many white northerners, who, viewed it as an exotic locale. Touristic observers, and self-proclaimed missionaries made excursions there to more closely observe the activities particularly of poor whites, whose sexual activities threatened the civilized status of the U.S. South, and jeopardized the American imperial prerogative abroad. The turn of the century proved to be a significant moment when the welfare and well being of the South was deemed crucial to the nation's health. Liberal social reform and imperial expansion were mutually constitutive. Northern white neo-abolitionists, concerned about degeneration and waning Anglo-Saxon ascendancy, a weak labour force and economic problems generated by the South, moved to incorporate poor southern whites (but not blacks) into the modernizing nation.

Modern U.S. nationalism took shape within an international crucible of empire building, and northern and southern white reformers extended surveillance to sexualized contact zones to police miscegenation, and illegitimacy. In 1921 the State of North Carolina launched an investigation into the conditions in an indigent white bootlegging community, resulting in a government report, "Swamp Island – A Study of Conditions in an Isolated Section of North Carolina." The "loose morals" of the many unmarried mothers challenged the racial order in a community that was "not straight" (marked as incapable of self-government), provoking surveillance strategies to protect the nation. A government official took "Kodak pictures" of the children to document the alleged immorality of their mothers.

The Superintendent of Public Welfare would forcibly remove seven children, placing them in State juvenile reformatories for normalizing education in civilization and good citizenship. Juvenile reformatories cultivated governable, productive individuals, capable of self-mastery, and self-surveillance. The Swamp Island bulletin provides a paradigmatic case of biopolitical state surveillance and intervention, offering a rare glimpse into the lives of those selected for institutional

moral uplift, attended by eugenic sterilization. The roots of current neoliberal discourses of responsibilization can be seen in early twentieth century juvenile reformatories that normalized "self-control" and "good citizenship".

While regarded as American, the U.S. South was marked as a quasi-colonial, retrograde space. Civilizationist rhetoric drew attention to the similarities between the region and transoceanic locales at the peak of empire. I consider the relationship between the South and the nation in a wider context, with consideration given to the complex intersecting regional, national and transnational discursive practices. In this paper, I use a combination of surveillance studies (governmentality, biopower) and postcolonial studies, including scholarship on human zoos, to examine practices of racialization and white southern belonging in the late-nineteenth and early twentieth century United States. I argue that racism was integral to the biopolitical state, and northern surveillance expedited the reinscription of white supremacy under imperial modernity.

Democracy

The Surveillance Society: Is Big Brother Watching You?

Session: **PARALLEL SESSION 9** – **Democracy I**

Date and time: **26th April 2014. (09:15-10:45)**

Author: **Saif Haq**

This paper provides an assessment of surveillance society as a national security challenge. It begins by sharing the key technological advancements and historically pertinent events that have led to the rise of the surveillance society. It touches on three emerging forms of surveillance, namely: social media surveillance, commercial surveillance, and sousveillance. Finally, it discusses some of the issues and implications that arise in a surveillance society, and highlights the impact of surveillance on the Singapore landscape based on examples drawn from other societies.

Counter-Democratic Surveillance -The watchful eye of a local institution

Session: **PARALLEL SESSION 9** – **Democracy I**

Date and time: **26th April 2014. (09:15-10:45)**

Author: **Morten Hjelholt**

Democratic theorists have long argued that active vigilant citizens, who watch over the state, as society's watchdogs, strengthen democracy. The image of the watchful eye of the people has been a central and contrasting image to the dystopian Orwellian image of Big Brother. It employs control mechanisms similar to those described by Foucault, but in the service of society. From this perspective democracy is seen as a composite of two realms – a sphere of electoral representation and a constellation of counter-democratic organizations – in constant tension with each other (Rosanvallon 2008). The watchful eyes of counter-democratic organizations are particularly made powerful by the rise of the Internet with its spontaneous adaption of watchful functions. However increased awareness and mistrust have led not to broader participation in traditional liberal institutions but to a greater social attention and demand for transparency of information. This paper takes a closer look at dynamics of counter-democratic surveillance from the perspective of a local political institution. The paper reports on a 3-year research project on counter-democratic functions of institutional oversight and organised distrust. Even though Government officials, over the three years of research, seemed to expand their overseeing legitimacy e.g. through the use of "Big Data" techniques, local institutions continued to inspect, monitor, investigate and evaluate the actions of

Government. Local accounts were created in the interest of the national overseers but correspondingly given as responds to fulfill legal requirements or more loosely defined public concerns. Consequently the watchful eye of a local institution form a counter-democratic sight aimed at the strategic intentions of the Government. The paper introduces the concepts of vigilance, denunciation and evaluations to explain how counter-democratic surveillance is often an overlooked feature when portraying surveillance as part of democratic promises and problems.

The Democratic Curve: Internet Technology and Surveillance/Sousveillance

Session: **PARALLEL SESSION 9** – **Democracy I**

Date and time: **26th April 2014. (09:15-10:45)**

Authors: **Michael Dahan and Mouli Bentman**

Does the internet promote democratic values? Does it empower citizenries and publics? Does the emergence of more sophisticated surveillance/sousveillance technologies jeopardize or fortify democracy, or simply strengthen reigning hegemonies? While the field of internet research is relatively young these questions seem almost ancient, having been raised from the very early days of net research. Yet, in spite of the vast body of research in these areas, we feel that these questions still lack a more comprehensive theory. Many of the scholars in this area tend to answer these questions in one of three ways, and in a typically dichotomic manner, showing that these new technologies are either an asymmetric tool of control that endanger democracy and liberty or on the other hand show it to be a symmetric tool for liberation and democratization. The third approach, often contend that due to the internet and surveillance/sousveillance technologies, influence on the political arena is limited, because the same old suspects control it, and that contrary to the utopian and dystopian views, the reality is much more banal. These researchers are inclined to promote the idea of “business as usual”.

In this paper we hope to show that the matter is more complex, and that although we can find various reasons and evidence to adopt either approaches, a closer look at the influences of the internet and the various surveillance/sousveillance technologies on democracy and democratization is necessary, and these need to be examined on a comparative scale, from authoritarians regimes to advanced liberal democracies. By creating a key that can assert the positive and negative impact of these technologies on democratic values we will show that to a certain extent, new surveillance/sousveillance technologies help to promote democratic values in authoritarian regimes or non liberal democracies while at the same time can be damaging beyond a

certain level of democratization. This effect creates a "democratic curve" that enables us better understanding of the relationship between technology and democracy. A comparative approach, as we apply in this initial research provides a greater depth of understanding regarding the affects of surveillance and sousveillance technologies on democratic and non democratic structures and publics.

Knowing how you vote before you do: micro-targeting, voter surveillance and democratic theory

Session: **PARALLEL SESSION 10** – **Democracy II**

Date and time: **26th April 2014. (11:00-12:30)**

Author: **Colin Bennett**

This paper surveys the various voter surveillance practices recently developed in the United States, assesses the extent to which they have been adopted in other democratic countries, and discusses the broad implications for privacy and democracy. Five interrelated techniques are analyzed: the development of voter management databases; the integration of personal data from commercial data brokerage firms; micro-targeting; the decentralization of data to local campaigns; and "targeted sharing" through social media. Structural and cultural differences between the United States and other democratic countries prevent the extensive and direct export of many of these practices. Yet issues about inappropriate communications from parties, about the sharing of data across systems, about intrusive uses of the Internet and social media, and about data breaches have surfaced in some countries. Furthermore, trends in Western party systems towards a greater de-alignment of the electorate will surely place further pressures on parties to target voters outside their traditional bases, and to find new, cheaper, and potentially more intrusive, ways to influence their political behavior. This paper builds on previous research to consider the theoretical tensions between concerns for excessive surveillance, and the broad democratic responsibility of parties to mobilize voters and increase political participation. These issues have been insufficiently studied in the social science literature. They are not just confined to the privacy of the individual voter, but relate to broader dynamics in democratic politics.

The changing notions and perceptions of state surveillance and their relation to political participation: an interdisciplinary, mixed-method study

Session: **PARALLEL SESSION 10** – **Democracy II**

Date and time: **26th April 2014. (11:00-12:30)**

Author: **Dimitris Tsapogas**

Only a number of U.S.-based studies have tried so far to understand the relationship between state surveillance perceptions and political participation. In addition, despite the well-known theoretical and empirical connection between surveillance and individual, non-political behavior, research on political participation rarely incorporates government surveillance into individual-level empirical models (Best and Krueger 2011). The small amount of literature that is available on the subject contains sometimes opposing and mixed views, when it comes to state surveillance.

My PhD research focuses on the changing notions and perceptions of citizens regarding state surveillance and the implications for offline and online political participation. This research seeks to answer how and to what extent does state surveillance modify citizens' willingness and behaviour in the context of political participation. The country of Greece was used as a European case study and all empirical data were collected from Greek respondents. Greece has had a long authoritarian surveillance legacy that aimed at socio-political control (Samatas 2004, 2005). Moreover, in a number of European surveys, Greek respondents appeared to show the highest levels of concerns about data protection, the highest levels of worries about leaving personal information online (Flash Eurobarometer No 225) as well as particularly low levels of trust in democracy, the government, the parliament and the police (European Social Survey 2010). Also, due to the on-going economic, political and social crises in Greece, civic and political participation are of crucial importance, constituting Greece as an important case study to focus on.

Drawing on a mixed mode, national survey and a series of focus groups and interviews that recruited participants from the whole political spectrum, this paper is discussing the results of this study and is presenting a methodological framework and theoretical model that can be tested across other countries.

Democratising surveillance?

Session: **PARALLEL SESSION 10** – **Democracy II**

Date and time: **26th April 2014. (11:00-12:30)**

Authors: **Paul De Hert and Rosamunde Van Brakel**

The relationship between surveillance and democracy is paradoxical and complex (Haggerty & Samatas, 2010). Surveillance can challenge democracy, be undemocratic but can also be democratic and empower democratic practices (Sclove, 1995, Monahan, 2010); authoritarian and democratic technologies exist simultaneously (Mumford, 1964). Technologies are inherently political and flexible "in the dimensions of their material form" and therefore, "their consequences for society must be understood with reference to the social actors able to influence which designs and arrangements are chosen" (Winner 1980: 134). Furthermore, technologies "possess degrees of agency such that they do not simply uncover pre-existing truths but actively contribute to the creation of certain truth regimes (whether about innocence or guilt, trustworthiness or suspiciousness, value or liability, etc)" (Monahan, 2008: 218). Hence, in the governance of surveillance it is necessary to test how democratic the surveillance technologies are, taking into account the above-mentioned assumptions.

The paper explores in what ways it is possible to make surveillance technologies more democratic by proposing, apart from the rule of law test, which currently exists in Europe, a rich democratic test to assess if surveillance technologies are democratic. This test would on the one hand consider if surveillance technologies are designed and implemented in a democratic way and on the other how the technologies have an impact on democracy.

Haggerty, K.D. & M. Samatas (2010) Surveillance & Democracy. New York: Routledge Cavendish

Monahan, T. (2008) Editorial: Surveillance and Inequality, Surveillance and Society, 5(3): 217-226.

Monahan, T. (2010) Surveillance as governance: Social inequality and the pursuit of democratic surveillance pp. 91-110 in K.D. Haggerty & M. Samatas, Surveillance & Democracy, New York: Routledge Cavendish.

Mumford, L. (1964) 'Authoritarian and democratic technics',Technology and Culture, 5(1): 1-8.

Sclove, R.E. (1995) Democracy and Technology. New York: Guildford Press.

Winner, L. (1980) Do Artifacts Have Politics?, Daedalus, 109: 121-36.

History

Unveiling the Archives of the Brazilian Dictatorship (1964-1985): Surveillance in the "Years of Lead"

Session: **PARALLEL SESSION 1** – **History**

Date and time: **24th April 2014. (10:30-12:00)**

Authors: **Lucas Melgaço and Ricardo Medeiros Pimenta**

Almost fifty years ago, Brazil suffered a coup d'état led by military officers with the support of conservative groups of the civil society. The dictatorial regime brought along a surveillance structure never before seen in the Brazilian history. Individuals and groups considered to be "subversive" were closely monitored. Data was constantly gathered, organized, classified and shared within a surveillance network instituted by the military. This database was used to justify the persecution, disappearance and even death of many Brazilians. On November 18, 2012, the Brazilian Chamber of Deputies created the National Truth Commission (Comissão Nacional da Verdade) with the aim of unveiling these abuses committed during the dictatorial regime. The archives created by this surveillance structure that once served to control the population are now helping to identify and bring to light the perpetrators of such violence. By analysing the reports of this commission, this work intends to highlight the dialectic aspect of information: it at the same time saves and kills, cares and controls. The once watched population is now watching their former watchers.

Surveillance in the former GDR: Objectifying suspicion - Suspicious objectivity

Session: **PARALLEL SESSION 1** – **History**

Date and time: **24th April 2014. (10:30-12:00)**

Author: **Olga Galanova**

Based on the recording of wiretapped phone conversations State security service of the former GDR (Stasi) has produced a huge amount of textual reports on persons being under the Stasi observation. These reports show various degrees of detailedness, ranging from condensed observational notes to meticulous transcripts. My paper deals with the question how these differences in the detailedness of Stasi protocols can be accounted for. It will be argued that the production of Stasi protocols had to cope with a basic conflict. On the one hand suspicion was the

initial ground for Stasi's decision to observe and wiretap a certain person; and suspicion remained a driving motive in the production of protocols and files. On the other hand the rationale of the very practice of observing and wiretapping was to "find" objective evidence for that which so far could only be suspected, thereby legitimizing the initial suspicion. The tension between suspicion and objectification was intensified by the fact that citizens of the GDR anticipated the surveillance by the Stasi and took countermeasures with the result that wiretapped but seemingly innocuous conversations stimulated all the more Stasi's suspicion. It will be shown that the documentary practices of Stasi protocols result from the conflicting relation between suspicion and objectification.

Ambivalent Faces: Visual Endeavours of Identification and Typification from 19th Century Science to Today's Biometric Recognition

Session: **PARALLEL SESSION 1 – History**

Date and time: **24th April 2014. (10:30-12:00)**

Author: **Raul Gschrey**

Starting with a historical perspective on techniques of identification, the paper will examine the ambivalent relationship of the seemingly mutually exclusive endeavors of identification and typification. In a second step I will try to trace continuities in the modes of visual production and analysis and provide a critical view on the often pronounced objectivity and neutrality of today's means of biometric recognition.

When in mid-19th century photography entered science as well as criminological and administrative practice it was widely perceived as an objective medium of depiction and was used as a means for identification as well as typification. Not only in visual anthropology, also in criminology, visual types became influential in the description and classification of the human body and face. A notable example, now perceived as "pseudo-science", is the technique of composite portraiture that was developed by the Victorian scientist Francis Galton in late 19th century. In his superimpositions of faces he explored the visual characteristics of the archetypal criminal, but also conducted experiments on "health" and "beauty". His visual constructions could be read in terms of what the German Media Studies scholar Dieter Mersch has described as "artificial visualisation". Galton's contemporary Alphonse Bertillon on the other hand has worked on the individualization of human appearance through biometric measurements and visual depiction. Drawing on Quetelet's social statistics, the French criminologist developed a technique, called "bertillonage" after its inventor, that allowed for the flawless identification of individuals through their physical characteristics and that was soon adopted by police agencies worldwide. The triumph of Bertillon's

method was eventually ended by the introduction of fingerprinting as a more manageable method of identification, which again was promoted and further developed by Francis Galton.

Today endeavours of identification move back to the face as the most visible part of the human body. Biometric facial recognition systems revolutionise identification, as for example in automated passport controls at airports. Face recognition systems in public space have reached trial stages in Germany and other countries. These systems will eventually allow for identification in passing, without the consent and often without the awareness of individuals. These asymmetries are further strengthened by laws that prohibit hiding the face in public.

Looking back at the origins, it becomes obvious that the techniques and modes of depiction are intrinsically connected to the developments in late 19th century. But in how far did these understandings and world-views influence today's techniques of identification? And in how far do ambiguities between identification and typification surface even today?

Mandated Categories: National Registration and Identification Technologies Under the British Mandate of Palestine 1917-1948

Session: **PARALLEL SESSION 1** – **History**

Date and time: **24th April 2014. (10:30-12:00)**

Author: **Scott Thompson**

Between 1917 and 1948 the region of Palestine was governed under the legislation of the British Mandate of Palestine (Council of the League of Nations 1917). Although the British government had been charged since 1917 to control immigration and citizenship within Palestine, the surveillance of the peoples of the region was expanded on June 18th 1936. As part of this expansion, the government of Palestine initiated a voluntary registration of its population and the issuance of individual Identity Cards. Although participation in the National Registration program was not mandatory under the British created and enforced laws, identity cards were required in order to enter certain controlled areas and to obtain access to certain government services. These identity cards were also used in the British organization of the sale and allocation of land.

In addition to data regarding the individual's name, appearance and place of residence, the UK's Palestinian register and ID system also highlighted individual "racial" and religious data – distinguishing the "races" of "Christian," "Jew," and "Arab." Furthermore, registration data also denoted certain types of people as "notables" (such as Imams) allocating to them differential rights under the laws of the Mandate. Soon after the cards were created they were also adopted by private industry, as corporations such as Shell Oil of Palestine required all entering their territories

to be properly registered, and certain business districts throughout Palestine could not be accessed without presenting one's identity card at government checkpoints.

This paper investigates the identification technologies, strategies and policies adopted by the British government in order to govern the population of Palestine during the British Mandate period. In particular, it will focus on the classifications of "race," gender, religion and occupation as a means of developing an understanding of the purposes for which these technologies were adopted, how they were developed, and the social impact that these technologies had on those who were categorized.

Identity

Surveillance and Identity – An Abstract Analysis

Session: **PARALLEL SESSION 3** – **Identity**

Date and time: **24th April 2014. (14:45-16:15)**

Authors: **Victoria Wang and John Tucker**

Surveillance practices are based on technologies that collect, store and process data, especially personal data. In this article, we offer a theoretical analysis of surveillance focusing on identity that covers a wide range of case studies. We find a set of concepts that can be used to model most forms of surveillance. We formulate: (i) an abstract definition of surveillance that works in both the physical and virtual worlds; and (ii) an abstract definition of identity that apply to people and objects. The definitions are intended to capture and structure the essential ideas that are common to the disparate surveillance situations of control, social sorting and mutual monitoring (Lyon, 2007). We define a surveillance system to consist of the following components and methods:

1. Entity. Entities that are people or objects that possess behavior in space and time;
2. Observable behavior. Methods for observing and recording behaviors;
3. Attribute. Methods for defining and recognizing attributes of behaviors, based on rules, norms, practices, and other observable properties;and
4. Identity. Methods for generating data that identify entities which exhibit the attributes and locate them in space and time.

Individuals have multiple identities, real and virtual, that are used in different aspects of their lives. Since many aspects of life are subject to surveillance, the notion of identity needs to be theorized. We argue that the notion of identity is fundamental to surveillance. We propose that identity is essentially a matter of data and define identities by means of data which we call identifiers. Our theory of identity illustrates the creation, provenance and transformation of identifiers. The analysis is very general and, at the same time, sufficiently precise to be formally articulated using algebra and logic in the sequel to this article.

Surveillance and Identity – A Formal Model

Session: **PARALLEL SESSION 3** – **Identity**

Date and time: **24th April 2014. (14:45-16:15)**

Authors: **Victoria Wang and John Tucker**

Surveillance is a general social phenomenon whose ubiquity is largely due to software technologies for gathering and processing data.In another submission, Wang and Tucker (2013), we argue that identity is fundamental to surveillance and formulate: (i) a general definition of surveillance that works in both the physical and virtual worlds; and (ii) an abstract definition of identity that apply to people and objects.

In this article, we formalise these concepts using the methods of algebra and logic. The mathematical model is illustrated with some disparate examples, arising from Lyon's (2007) three categories of surveillance. We are able to give formal definitions of ideas such as social sorting. Our model emphasizes an important, if neglected, component idea of surveillance, namely the identity of the people or objects observed. Identities are defined by means of identifiers, which are data designed to specify the identity of an entity in some particular context or for some purpose. Since there are many situations in need of identifiers, there are many identifier management systems. In our model, we assume that entities are known only through their identifiers. We examine the creation, provenance and transformation of identities, investigating how identifiers depend upon other identifiers. We represent the provenance of identifiers by identity trees – the leaves of which are personal identifiers. Indeed, surveillance ultimately directs its attention to individuals. The changes of identity and detection of identity are modelled by mappings that transform or reduce one identity management system to another. We examine the subtleties involved in defining personal identifiers that refer to a unique human being. Finally, we reflect on the role of formal methods to theoretical give insights in sociological contexts.

References:

Lyon, D (2007). Surveillance Studies: An Overview, Polity Press.

Wang, V. & Tucker, J.V. (2013). Surveillance and Identity – An Abstract Analysis, submitted.

Control by a government to the citizen through a national identification number system - in the case of Japan

Session: **PARALLEL SESSION 3** – **Identity**

Date and time: **24th April 2014. (14:45-16:15)**

Author: **Yutaka Kusajima**

In May 2013, the bill of national identification number system was approved in Japan. Government appeals that we need this bill for both taxation and social security. This bill realized three features, to make common unique numbers, legalization of data matching and identification by use of ID card. In Japan, we have discussed a national ID number system from 1960's. Government has planned to introduce such a system at various times, but by protests of people, it failed or produced only incomplete system. But the bill of national identification number system has approved and completed the three features as above.

Many actors in politics, economy and bureaucrat has discussed such a system and planned to introduce it. The point of discussions were improvement in productivities, taxation system and social security. In 1960's Japan was at a rapid economic growth by the state leadership, and the idea of office automation was introduced. State leadership means leadership by bureaucrat. Under efficiency strategies by computer technologies, there is a thought that excellent bureaucrats enable to lead Japan to the right path. At that high economic growth time, number system intend to correct tax from rich people or company, and now, at the low economic growth and low birth rate, it intend to control balance sheet of state. Government appeals that this system enable to supply necessary service to whom needs it exactly. But it means that political power can be used to the specific people through specific actions. We have to take notices that there is a thought of control to the citizens in this background. And this system is a tool to consolidate the power, and brings to consolidate surveillance and control to citizens. A national identification number system is a tool for 'smart' surveillance system with developed information and communication technology.

Terror(ism)

Unthinking Extremism – Radicalizing Narratives that Legitimize Surveillance

Session: **PARALLEL SESSION 3** – **Terror(ism)**

Date and time: **24th April 2014. (14:45-16:15)**

Author: **Ben Harbisher**

While key events such as 9/11 and 7/7 justified the call for more adept forms of intelligence, they led to sweeping changes to criminal legislation in Britain, that remain contentious for the subsequent reforms they have evoked.

Strategies such as CONTEST and RESILIANCE have permitted the Government to widen existing definitions of terrorism to include protestors, subjecting campaigners to unprecedented levels of surveillance during peaceful demonstrations.

To put the depth of this surveillance into context, the monitoring of protesters significantly exceeds conventional public surveillance in the UK. In a nation which boasts over 4 million CCTV cameras on the streets, there is more surveillance, used in greater depth and with more regularity during demonstrations.

The entire range of surveillance logistics are employed during public order actions. These include personal searches, ANPR, Communications Interception, Covert Human Intelligence Sources, Databases, Spotters Cards, Video or Photography, and even Bureaucratic Surveillance.

In a regulatory context, resounding similarities now exist between terrorism and direct-action. Public demonstrations are listed as an equivalent threat to domestic services in almost every piece of counter-terrorism literature, allowing the security services to work towards an ultimate goal of pacification and control.

At a strategic level, both activism and terrorism have been rebranded as extremism – which has become an all-purpose euphemism for any act of violence the state does not condone. The term has come to legitimise the disproportionate use of surveillance against protestors, and significant attention must be paid to both its use and its origins.

Organisations such as ACPO-TAM and the RICU are responsible for disseminating these strategic narratives into the public domain. The shared nomenclature of extremism is indicative of counter-subversion thinking and is used to undermine the factors leading to radicalization. However, extremism discourses also serve to reduce public sympathy for protestors – legitimizing unrestrained surveillance.

Fusion centers and joint databases in Germany: Function creep and the elusive accountability of sharing counterterrorism intelligence

Session: **PARALLEL SESSION 3** – **Terror(ism)**

Date and time: **24th April 2014. (14:45-16:15)**

Author: **Eric Toepfer**

With the new paradigm of networked security fusion centers are emerging in the U.S. and Europe as focal points for sharing data and intelligence across security agencies (Stanley 2007, Monahan & Regan 2012, Belgian Standing Intelligence Agencies Review Committee 2010). Initially created to combat terrorism these centers are reported to quickly pursue an all-crime approach while being elusive to democratic oversight and accountability.

In Germany the Joint Counterterrorism Center (GTAZ) was launched as the first national fusion center in 2004. In the meantime additional fusion centres have become operational at the national and regional level (Töpfer 2013). Bringing together law enforcement, intelligence services and other government agencies these hybrid fora aim to facilitate the sharing of information, bolstered by joint databases.

The paper will provide an overview of the development and current landscape of German fusion centres and will discuss how existing privacy legislation is shaping their evolution and operation.

References:

Belgian Standing Intelligence Agencies Review Committee (ed.) (2010): Fusion Centers Throughout Europe. All-Source Threat Assessments in the Fight Against Terrorism. Antwerp etc.: Intersentia.

Monahan, Torin & Priscilla Regan (2012): Zones of Opacity. Data Fusion in Post-9/11 Security Organisations. In: Canadian Journal of Law and Society, 27 /3), pp. 301-317.

German, Michael & Jay Stanley (2007): What's Wrong with Fusion Centers? Washington D.C.: ACLU.

Töpfer, Eric (2013): Informationsaustausch zwischen Polizei und Nachrichtendiensten strikt begrenzen. Konsequenzen aus dem Urteil des Bundesverfassungsgerichts zur Antiterrordatei. Berlin: Deutsches Institut für Menschenrechte (Policy Paper No. 21).

Understanding the Uneven Impact of Counter-Terrorism: An EU Case Study

Session: **PARALLEL SESSION 3** – **Terror(ism)**

Date and time: **24th April 2014. (14:45-16:15)**

Author: **Fiona de Londras**

It is widely accepted that counter-terrorism, including surveillance, impacts on different people and groups differently. However, neither the full meaning of 'impact' nor the range of uneven impacts are fully understood in the context of counter-terrorism. This paper presents findings from a major FP7-funded research project entitled SECILE (Securing Europe through Counter-Terrorism: Impact, Legitimacy and Effectiveness) that aims, inter alia, to develop a more complete understanding of the nature of counter-terrorist impact. It draws on the disciplines of law, sociology, security studies and political theory, and on empirical work undertaken within the project, to propose impact indicators and demonstrate scales of unevenness.

Surveillance, Militarization, and the (Re)construction of Canadian Democracy

Session: **PARALLEL SESSION 3** – **Terror(ism)**

Date and time: **24th April 2014. (14:45-16:15)**

Author: **Mohammed Masoodi**

Since the inception of the 'war on terror', Canada has been among the group of Western democratic countries that have extensively depended on militarization and subsequently relied more heavily on surveillance technologies to monitor its citizens in the name of security. It can be contended that the purpose of surveillance technologies and the militarization of Canadian society post-911, is a precursor to greater government control; constructing ideal citizens that are 'governable' and can benefit the government by giving up certain freedoms, supporting government initiatives aimed ostensibly at securing citizen safety. This logic fits in nicely with narratives that argue there is no end to the 'war on terror' and therefore countries like Canada will continue indefinitely to militarize and rely on surveillance technologies. This proposed paper will examine sociologically the relationships between on the one hand, popular discourses and practices of militarization, and on the other, the adoption of surveillance systems whose software and hardware have become routine aspects of negotiating everyday life for all citizens. While government uses such risk management knowledge to seek security, social and other inequalities tend to be reproduced. This paper will investigate the effects of Canadian political discourses surrounding militarization as the site for government control on the construction of Canadian society. Using a

critical discourse analysis (CDA) framework, the rise in militarization, its links with surveillance, and its effects on the reconstruction of Canadian democracy will be investigated.

Resilience

Taking 'Resilience' Seriously: Exploring its Implications in the Surveillance Context

Session: **PARALLEL SESSION 4** – **Resilience**

Date and time: **25th April 2014. (09:15-10:45)**

Authors: **Charles Raab, Richard Jones and Ivan Szekely**

'Resilience' is a fashionable but contested term in social, governmental and business discourse. It is normally used without defining its properties or how it relates to other terms that characterise processes or states of being. In the face of man-made and natural disasters, it normally has positive connotations, and both individual and collective frames of reference. This paper explores the general concept of 'resilience' on the plane of abstract analysis, and then uses it specifically in the context of responses to surveillance. It does this by developing new models and by extending existing ones in a more precise manner that can describe resilient processes as they unfold over time and in anticipation of, or reaction to, adversities of different kinds and severity. Societies deploy resilient strategies against shocks or stresses that are brought about by terrorism, crime, and other causes. These strategies may include surveillance, a phenomenon that – as a source of adversity itself – may paradoxically invite resilient activity whether precautionary or in mitigation of the harms caused by surveillance. This paper thus focuses upon surveillance as a specific focus for developing and applying its conceptual analysis and modelling of situations, and for evaluating contemporary developments in 'surveillance societies'.

Culture and Ethics of Resilience in Italy

Session: **PARALLEL SESSION 4** – **Resilience**

Date and time: **25th April 2014. (09:15-10:45)**

Authors: **Chiara Fonio and Alessia Ceresa**

While the concept of resilience has been broadly analyzed in relation to, inter alia, the fields of crisis management (Arjen, McConnell 2008), urban studies (Coaffee, Murakami Wood, Rogers 2009) and security studies (Coaffee 2008; Aldrich 2010), the politics of resilience within the area of "surveillance studies" (Ball, Haggerty, Lyon 2012) have yet to be conceptualized. This lack of analysis has led surveillance scholars to focus more on politics of resistance (Fernandez, Huey 2009) than on politics and practices of resilience in relation to surveillance technologies.

The first part of this contribution is an attempt to focus on the relationship between resilience and surveillance through a sociological perspective drawing from both security and surveillance studies. In particular, this paper looks at if and how resilience emerges in contemporary surveillance societies where the notion of democracy is often challenged by regimes of visibility (Brighenti 2010) that are clearly non-democratic. In this context, many questions need to be addressed. For instance, what is resilience in today's surveillance societies? Are there resilience options? What are the differences between resistance and resilience in relation to surveillance?

In the second part a specific emphasis is given to a case study focused on the dynamics of surveillance and resilience in Italy. Despite the growth of video surveillance in Italy has been "silent" (Fonio 2011), publicly owned surveillance cameras are used almost everywhere. This part is concerned either with cities which seem to be more "resilient" to video surveillance or with social actors (individuals or groups) who have dealt with the proliferation of CCTV through a "resilient approach". The "Anopticon" project, carried out in the city of Venice, is analyzed as it sheds light on politics of resilience to surveillance cameras and offers insights on ethical dimensions and power relations.

Resilience in a surveillance society

Session: **PARALLEL SESSION 4** – **Resilience**

Date and time: **25th April 2014. (09:15-10:45)**

Authors: **David Wright and Reinhard Kreissl**

Our paper focuses on resilience in a surveillance society. The paper is in six main parts.

The first part, "Defining a surveillance society", includes definitions (e.g., from the SSN Report on the Surveillance Society done for the UK Information Commissioner and the follow-on reports from committees of the UK House of Commons and House of Lords), and manifestations of today's surveillance society. It characterises tomorrow's surveillance society.

The second part considers how surveillance can be used to protect society, e.g., against crime and terrorism, but also more minor offences such as fraudulent benefit claims.

The third part considers how surveillance can undermine the very freedoms and values it aims to protect, notably such as privacy, trust, dignity, autonomy, freedom of movement, freedom of thought and expression, freedom of association, freedom of information, freedom from discrimination, equality of treatment, rule of law and due process, presumption of innocence, right to lawful protest. The paper provides examples in each case.

Part four addresses the question of what it means to be resilient in a surveillance society. It looks at how the term resilience is used in different domains, and how the term has evolved. It also assesses the extent to which we can draw on these different definitions for applicability in surveillance. The paper then responds to questions such as: Whose resilience? Is resistance a resilience strategy or are resilience and resistance different things? The next section says how the authors interpret resilience in a surveillance society, which is followed by a section on surveillance and power.

Part five identifies measures to increase resilience in a surveillance society. It includes political and regulatory measures, such as accountability and oversight, other privacy principles, “drawing lines”, and awareness and communications. In addition, it identifies societal and individual measures.

Part six draws conclusions on resilience in a surveillance society.

Police

Policy, design and use of police- worn bodycams – a case study from the Netherlands

Session: **PARALLEL SESSION 4** – **Police I**

Date and time: **25th April 2014. (09:15-10:45)**

Author: **Tjerk Timan**

In the Netherlands, police-worn bodycameras (the bodycams) have been tested and deployed since 2009. Their introduction followed after rumours of positive test results of bodycam practices in the UK. Although this camera is single-purpose in the sense of functionality (to record the moving image), its use is multiple; evidence gathering on crime scenes, surveillance by bikers with cameras, police officers on foot with bodycams1. The latter two types of use are under investigation here, since they are the two modes witnessed in Dutch nightlife districts. The question is how this bodycam made its introduction in surveillance practices in these districts. What does this new surveillance artifact do in use practice and how did it come into being in the particular way it is now?

I will focus on three groups of actors that are involved in the development and use of the bodycamera in the Netherlands and look at them through the heuristic lens of objectual practices(Knorr-Cetina, 20012) of the bodycamera. Firstly, policy makers and the places where needs and regulations (in other words, design requirements) of the camera have been issued. Secondly, the designers of the camera will be addressed and the choices they made in both soft- and hardware development. Thirdly, I focus on practices of use by police officers to see how the bodycamera changes their work practice. Empirical material used to answer the research question entails policy documents, script analysis of the bodycamera and interviews and participatory observations in nighttime districts with police officers. Comparing these different actors, the paper aims to understand which meanings and practices of use of the bodycamera are articulated and stabilized in Dutch nightscapes and how this alters surveillance practices

Familiar Suspects: surveillance images as intelligence and evidence in criminal trials

Session: **PARALLEL SESSION 4** – **Police I**

Date and time: **25th April 2014. (09:15-10:45)**

Authors: **Mehera San Roque and Gary Edmond**

This paper focuses on surveillance artefacts, primarily images, as investigative intelligence within the criminal justice system, and the use of such artefacts as evidence within the criminal trial. The proliferation of CCTV systems, combined with the now commonplace use of mobile phones and other communication devices, has produced a massive body of images that can be invoked in the attempt to identify those engaged in (potential) criminal activities; with both the prevalence, and reliance, likely to increase diachronically. Investigations into high profile crimes (such as the Boston bombing), and or mass disturbances (such as the London and Vancouver riots) are often accompanied by the strategic release of CCTV (or other) images by investigators. Investigations are often presented as being advanced by the crowd sourcing of surveillance material and by associates or relatives recognising and informing on those captured by cameras. High profile successes, in combination with public expectations in the technological capabilities of automated (facial) recognition systems, have generated renewed political and public enthusiasm for the extension of CCTV and other surveillance systems across public, quasi-public and private spaces.

Within surveillance studies, discussion of the proliferation of CCTV systems remains primarily concerned with the implications for the regulation of urban spaces or populations, privacy and human rights. Critical work points to the uneven development and (in)effectiveness of systems in terms of crime prevention and social control. Though, discussion rarely includes the criminal trial as an element within, or influence upon, the surveillant assemblage. With the rise in the reliance on images as evidence in criminal trials, we examine the increasing use of familiars to identify persons of interest, alongside the concomitant rise in the mediation of images by those claiming some kind of 'expertise' in reading images—usually to reveal identity. The rapid proliferation of surveillance artefacts (and imaginaries) has been matched by a ready conversion—by lawyers and judges—of often highly ambiguous images and supplementary opinions of unknown reliability, into admissible evidence and proof. This conversion has been indifferent both to the complexities of image interpretation, and to the inability of conventional trials—whether adversarial or inquisitorial—to expose and convey epistemic limitations. This paper extends the analysis of the knowledge economies that have accompanied the proliferation of visual monitoring, and the circulation of images, offering a critical response to the reliance on (familial) recognition as intelligence, and to

the non-reflexive and overly-accommodating evidentiary regimes developed by courts.

Sorting (out) youth; Transformations in police practices of classification and surveillance of cases of 'problematic youth groups'

Session: **PARALLEL SESSION 4** – **Police I**

Date and time: **25th April 2014. (09:15-10:45)**

Author: **Vlad Niculescu-Dinca**

Drawing on ethnographic research in a police station, this paper explores a set of methodological and normative issues in technologically-mediated policing. It draws on data in The Netherlands where the prioritization of the issue of 'problematic youth groups' on the public agenda entailed a proactive approach to sort out the problems generated by these youth. The approach concentrated so far on 'criminal' groups but is set to focus more on the much larger numbers of 'nuisance' and 'annoying' youth groups – sorted according to the police shortlisting method (Bureau Beke 2009). Although group numbers dropped in national statistics (Bureau Beke 2013), the approach promotes early signalling to prevent them 'slip down to the status of a criminal group' (Van Montfoort /Office Alpha and Dutch Youth Institute 2013). This includes geographical mapping of their activities as well as internet and social media monitoring (SMM).

Analytically, the paper adopts an ANT approach (Akrich and Latour 1992, Bowker and Star 1999, Law 2009) to understand how their problematic and suspicious character is constructed. Additionally, it analyses a dedicated police solution, which is set to enable automatic collection of social media information. The solution is built with 'the idea of 'privacy by design' from the start' to restrict the monitoring of internet and social media activity only to specific 'cases' (interview main designer 2012).

Taking a performative understanding of social science method (Law 2009), the paper first raises a set of questions about the statistics on cases of 'problematic youth groups' and about the very police definition of 'youth group'. Linking these with developments in SMM technologies, the paper shows next that particular alignments of technological, organizational and policy factors legitimize the automatic data gathering in a multitude of cases. This analysis of the issue of 'problematic youth groups' shows that even with restrictions built in design, particular implementations of the notion of 'case' play a pivotal role in police surveillance practices and their information gathering processes. As it turns out, cases can be vaguely defined and easily extended in the use context, with direct influence on what and how much data is legally stored.

Shifting paradigms. Electronic monitoring in Belgium

Session: **PARALLEL SESSION 5** – **Police II**

Date and time: **25th April 2014. (11:00-12:30)**

Authors: **Kristel Beyens, Marijke Roosen and Sonja Snacken**

Electronic monitoring (EM) became operational in Belgium in 2000 and has known periods of instability ever since it was put in practice. We are currently witnessing a shift in EM practices in Belgium, which can be seen as the result of a shift in the underlying penal paradigm and political pressures for 'truth in sentencing' and credibility. Initially, the so-called 'Belgian model' was characterized by a balance between social support and control. The current penal practice is however characterized by a diminished or total withdrawal of social support and more emphasis on mere surveillance. This evolution is however not unique for Belgium.

This paper will first describe and critically analyse the current developments in the field of EM in Belgium. New practices are being applied, supported by new technologies. Moreover, a shift in the EM paradigm is associated with a shift in the penal actors' tasks. Where the probation officer was formerly an important actor in the field of EM, his tasks are being reduced and the 'monitoring officer' comes more to the fore. These monitoring officers operate with a different mission and have a different educational background than the probation officer, with less or no emphasis on social work principles. These professionals operate with less discretion, as the procedures are becoming more standardized.

Secondly, we focus on the consequences of these evolutions for the relationships between the supervisor and supervisee and the encompassing 'nature' of the punishment. We hypothesize that these relationships become less personalized and even more virtual. Furthermore, the lack of discretion might lead to differences in the decision-making processes, for example with regard to compliance.

Electronic Surveillance and Penal Innovation Across Europe

Session: **PARALLEL SESSION 5** – **Police II**

Date and time: **25th April 2014. (11:00-12:30)**

Author: **Mike Nellis**

Using data from the Conference Permanenete Europeenne de la Propbation (the CEP) and the Council of Europe Council for Penological Cooperation, this paper will seek to document and explain the spread of the electronic monitoring (EM) of offenders – initially in the form of curfews

and home confinement – across Europe from the 1990s to the present day. It will note distinct patterns of development and use in western Europe, Scandinavia, and Eastern Europe (and the Balkans) and pay specific attention to countries which now seem anomalous because they have not developed national EM schemes, or actively resisted them. Against a backcloth of resurgent neoliberalism, and the normalisation of surveillance practices in many spheres of social life, the political, commercial and professional drivers of EM's development – including the recent advent GPS tracking technology – will be explored in terms of its implication for existing probation services, and an attempt made to assess its future prospects.

Exploring the Potential of Victim-Oriented Electronic Monitoring

Session: **PARALLEL SESSION 5** – **Police II**

Date and time: **25th April 2014. (11:00-12:30)**

Author: **Craig Paterson**

The increasingly psychological terrain of crime and disorder (perception) management in neo-liberal political economies has had a transformative impact upon governmental use of electronic monitoring (EM) technologies. Surveillance technologies such as EM, biometrics, and CCTV have flourished in commercial environments that market the benefits of asocial technologies in managing disorderly behaviour and which, despite often chimerical crime prevention promises, appeal to the ontologically insecure social imagination. The growth of EM in criminal justice has subsequently taken place despite a lack of evidence that it protects the public and reduces re-offending.

Innovative developments in Portugal, Spain, Argentina and the United States have subsequently re-imagined EM technologies as more personalised devices that can support victims rather than control offenders. These developments represent a re-conceptualisation of the use of the technology beyond the neo-liberal prism of rational choice theories and offender-oriented thinking. This paper identifies the socio-political influences that helped conceptualise first generation thinking about EM as, firstly, a community sentence and latterly, as a technique of urban security. The paper reviews attempts to theorise the role and function of EM surveillance technologies within criminal justice and explores the contribution of victimological perspectives to the use of EM 2.0.

Experimenting surveillance: between exceptionality and everydayness

Session: **PARALLEL SESSION 6** – **Police III**

Date and time: **25th April 2014. (13:30-15:00)**

Author: **Francisca Gromme**

In the Netherlands small-scale pilots with surveillance technologies are fairly common. A study of three crime control pilots reveals that these three projects had one thing in common: ambiguity. In these pilots new technologies were tested in everyday policing practices, such as the use of data mining to generate profile of 'problem youth'. I show that these projects both relied on a state of exceptionality, and on their 'everydayness'. Furthermore, they used the techniques of a 'theatre of proof' (Latour 1988) to convince audiences, while they shunned publicity at the same time. Finally, they both introduced a technology in a new environment and contained its effects.

This begs the question of what role pilots play in surveillance practices. I explore the idea that it is exactly the ambiguity and flexibility of these projects that facilitates their introduction and their diffusion (Mol and De Laet 2000). One of the problems with this mode of operation is the relative unaccountability of these pilot projects.

Neo-colonial vision: Plural Policing, Aboriginality and visual surveillance in two Australian towns

Session: **PARALLEL SESSION 6** – **Police III**

Date and time: **25th April 2014. (13:30-15:00)**

Authors: **Dean Wilson and James Martin**

Recent observation studies of surveillance camera control rooms have highlighted the importance of social and cultural context on the operation of visual surveillance. Moreover, ethnographic research examining the operation of visual surveillance has highlighted the location specific nature of particular security assemblages interacting with surveillance systems. Taking this work as its starting point, this paper is based upon ethnographic observation and semi-structured interviews with surveillance and security personnel in two Australian locations: 'Tropicville' and 'Region Town'. Both 'Tropicville' and 'Region Town' have significant populations of Aboriginal Australians. In both locales the surveillance, monitoring and control of Indigenous Australians in public space was a major focus of camera operators. However, the outcomes of such surveillance markedly diverged, dependent upon the particular configuration of security nodes in each location, and how these security nodes were shaped by local political factors. In particular, the degree of Aboriginal

participation within the security patchwork was instrumental in forging the subsequent nature of surveillance. While, within the context of Australia, visual surveillance always contains the potential to exacerbate neo-colonial patterns of marginalization and criminalisation, it can also operate on occasion with Indigenous self-governance that mitigates, although not entirely eliminating, the negative and racialized gaze of surveillance.

Policing Made Visible: Mobile Technologies and the Importance of Point of View

Session: **PARALLEL SESSION 7** – **Police IV**

Date and time: **25th April 2014. (15:15-16:45)**

Author: **Ben Brucato**

"Testimony is interesting. Video is compelling." So claims Taser's marketing materials for wearable cameras and content management software designed for police departments. This perspective is echoed among advocates for sousveillance of police. This paper explores how mechanical objectivity functions in the discourse in these two spaces. When the objectivity of visual surveillance media is placed in dispute, it punctuates two broad considerations. The first regards efficacy in institutional and popular efforts to render visible police power. Secondly, it speaks to the more general question of transparency.

Taser AXON Flex offers multiple wearable camera options, such as camera-integrated eyeglasses, and links with other devices like stun-gun mounted cameras in the web-based EVIDENCE.COM video database. Taser's communications about the AXON Flex system stress the importance of mobility in surveillance technologies and point-of-view in the media they produce. AXON Flex allows the cameras to move with officers, as opposed to commonplace dashboard cameras. EVIDENCE.COM allow in-the-field assessment of video footage on smart phones, tablets, and laptops. Crucially, the focus on point-of-view coincides with the juridical principle of reasonableness, which privileges officers' points of view in use-of-force investigations.

The emphasis on point-of-view is also a reaction to the explosive growth in civilian video documentation of policing, most commonly produced with video- and data-enabled smart phones. I compare how mechanical objectivity functions as a means similarly in the discourse of advocates for civilian sousveillance of police, but using different rationales.

In considering the conflicts over visual representations of police and policing, I explain the implications of this conflict for surveillance studies. I question whether we can legitimately assume visual surveillance is efficacious and powerful as a result of its objectivity. Seeing might be

believing; but it matters who is seeing what, and from whose perspective.

Privacy, photographs and the police: The role of the law in the "war against photography"

Session: **PARALLEL SESSION 7** – **Police IV**

Date and time: **25th April 2014. (15:15-16:45)**

Author: **Tj McIntyre**

Observers have identified the growth of a "war against photography" in which police throughout the world attempt to prevent photography in public spaces, particularly photography of the police themselves. The underlying motives vary – in some cases there are misguided fears that photographs may be "useful to terrorists" while in others there is a simple desire to avoid accountability and to conceal wrongdoing of police misconduct. Whatever the reason behind a particular restriction, the result is often that institutional surveillance continues unchecked while photography by citizens (sousveillance) is prevented and even criminalised. This paper will examine the legal issues presented by this war on photography and will consider how the law should respond. In particular it will consider whether a right to photograph in public can be characterised as an aspect of the right to freedom of expression and, if so, the ways in which the law should promote that right. It will consider the extent to which those photographed – particularly police – might enjoy competing privacy rights which would justify restrictions on photography. Finally it will consider whether laws intended to promote privacy may (whether inadvertently or deliberately) frustrate sousveillance as a tactic to hold institutions to account and will argue that greater attention should be given to power asymmetries in deciding on the creation and enforcement of privacy rights.

Compromised Trust: DHS Fusion Centers' Policing of the Occupy Wall Street Movement

Session: **PARALLEL SESSION 8** – **Police V**

Date and time: **25th April 2014. (17:00-18:30)**

Authors: **Torin Monahan, Krista Craven and Priscilla Regan**

State surveillance programs often operate in direct tension with ideals of democratic governance and accountability. The fraught history of surveillance programs in the United States, for instance, illustrates that government agencies mobilize discourses of exceptional circumstances to engage in

domestic and foreign spying operations without public awareness or oversight. While many scholars, civil society groups, and media pundits have drawn attention to the propensity of state surveillance programs to violate civil liberties, less attention has been given to the complex trust dynamics of state surveillance. On one hand, in justifying state surveillance, government representatives claim that the public should trust police and intelligence communities not to violate their rights; on the other hand, the very act of engaging in secretive surveillance operations erodes public trust in government, especially when revelations about such programs come to light without any advance notice or consent. In order to better understand the trust dynamics of state surveillance, this paper will analyze some of the competing trust relationships of Department of Homeland Security (DHS) "fusion centers," with a focus on the role of these organizations in policing the Occupy Wall Street movement of 2011 and 2012.

'No, no!' said the Queen. 'Sentence first - verdict afterwards.' A rhizomatic approach for understanding preemptive surveillance

Session: **PARALLEL SESSION 8** – **Police V**

Date and time: **25th April 2014. (17:00-18:30)**

Author: **Rosamunde van Brakel**

Increasingly surveillance technologies are designed to predict future crimes. Within criminological literature a shift has been emphasised from a post-crime to a pre-crime society (Fitzgibbon, 2004; Zedner, 2007; Harcourt, 2007; Hebenton & Seddon, 2009; McCullough & Pickering 2009; Van Brakel & De Hert, 2011). One of the main characteristics of this pre-crime society is the increased use of preemptive surveillance technologies for crime control and prevention such as for instance the use of predictive analytics and smart CCTV by law enforcement and the use of pre-crime databases of children by social workers.

The main purpose of this paper is to use a rhizomatic approach (Deleuze & Guattari, 1987; Haggerty & Ericson, 2000) in order to provide a better understanding of the nature of preemptive surveillance. By looking at the governance and practice of these types of systems as rhizomatic, surveillance dynamics, power relations and (un)intended consequences come to light that otherwise would have stayed in the dark. Moreover, this approach goes beyond the traditional understanding of surveillance as an exclusive asymmetrical relationship between the surveillance authority and the subject of the surveillance and it becomes clear how other actors, and especially technology play an important role as well.

Deleuze, G. & F. Guattari (1987) A Thousand Plateaus: Capitalism & Schizophrenia, London:

Athlone

Fitzgibbon, W. (2004) Pre-emptive criminalisation: risk control and alternative futures, London: NAPO ICCJ Monograph).

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

Harcourt, B.E. (2007) Against Prediction: Profiling, Policing, and Punishing in an Actuarial Age, Chicago: University of Chicago Press.

Hebenton, B. & T. Seddon (2009) From Dangerousness to Precaution. Managing Sexual and Violent Offenders in an Insecure and Uncertain Age, British Journal of Criminology, 49(3): 343-362

McCullough, J. & S. Pickering (2009) Pre-Crime and Counter-Terrorism Imagining Future Crime in the 'War on Terror', British Journal of Criminology, 49 (5): 628-645.

Van Brakel, R. & P. De Hert (2011) 'Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies', Cahiers Politiestudies 20: 163-92

Zedner, L. (2007) Pre-crime and post-criminology? Theoretical Criminology, 11 (2): 261-281.

Secret Manoeuvres in the Dark – Corporate and police spying on activists

Session: **PARALLEL SESSION 8** – **Police V**

Date and time: **25th April 2014. (17:00-18:30)**

Author: **Eveline Lubbers**

The exposure of undercover policeman Mark Kennedy in the environmental movement revealed how the state monitors political campaigns. My book Secret Manoeuvres in the Dark exposes a related threat to our political freedoms – undercover activities by corporations. Based on exclusive access to previously confidential sources, this research shows how companies such as Nestlé, Shell and McDonald's use covert methods to gather intelligence on campaigners, counter criticism, and evade accountability. Corporate intelligence gathering has shifted from being reactive to proactive, with important implications for democracy itself. Cooperation between the government and corporate intelligence in such secret operations is a seriously neglected field of research.

A corporation does not spy on its critics just to know what is going on, it does so to be prepared and to defend itself. The connection between surveillance and the gathering of intelligence on the one hand, and subsequent corporate strategy on the other, is crucial to understand what is happening and why.

The force of former police and intelligence staff now working for big business is a pertinent example of why labels such as 'conflict of interests' no longer suffice. Operating on both sides of the public-private revolving door, they continue to work to further a shared agenda. Their goals, as well as the political networks involved, urgently need to be mapped out and made transparent.

Undermining campaigners is essentially undermining democracy. The examples of corporate spying and strategizing in Secret Manoeuvres raise concerns about the 'engineering of consent.' The book details multiple means large corporations have at their disposition to manipulate public debates and to exclude the voices of their critics. Deliberative democracy requires the participation of civil society, but if campaigners and NGOs are sabotaged then the terms on which policy and political decisions are made is called into question.

City

Smart, Efficient, and Visible: Surveillance Technologies for Sustainable Cities

Session: **PARALLEL SESSION 4** – City

Date and time: **25th April 2014. (09:15-10:45)**

Author: **Baki Cakici**

When information and communication technologies are positioned as essential tools for tackling sustainability challenges, different surveillance methods commonly appear in their descriptions. In these discourses, homes and cities are smarter, energy distribution is adaptive, mobility is responsible yet unrestrained, and lifestyles are more sustainable. I investigate the paradoxical quest to achieve sustainability by developing highly advanced digital technological systems in several European initiatives that aim to create smart and sustainable cities. Using perspectives from science and technology studies and surveillance studies I ask: what is being sustained, and for whom?

Novel surveillance systems are proposed to aid the inhabitants of smart cities and smart homes in behaving sustainably, based on the assumption that behaviour can be changed using surveillance systems, coupled with a view of technology as a value-neutral vehicle for providing information to drive behavioural change. On the one hand, these systems allow human and non-human subjects to be governed at a distance by a central authority. On the other hand, they do not function according to their designers' intentions, and surveillance subjects exercise their own agency by resisting the watchful eye, or by shaping the technologies to suit their own needs. While recognising that climate change and environmental justice are, and will continue to be, significant concerns for contemporary societies, I question why surveillance is a highly prominent method in discourses of digital technological systems for sustainability. In conclusion, I suggest that the design and development of these systems stand to benefit from critical analyses by scholars in the field of surveillance studies, as these systems can potentially sustain unequal and unjust power relations, but they can also be effective tools for voicing social concerns.

Imagining the City: Synoptic Power, Emotion and Urban Governance

Session: **PARALLEL SESSION 4** – City

Date and time: **25th April 2014. (09:15-10:45)**

Authors: **Roy Coleman and Maria Angeles Martinez Serrano**

This paper presents the preliminary results for the Spanish case study on access rights within the framework of the EC-funded IRISS3 project.

The paper summarises the process and results of exercising the right of access in 30 sites based in Spain, in domains as broad as: health, transport/holidays, work, education, finances, leisure, communications, consumerism, and civic engagement. Within these domains, specific research sites were identified and approached.

The method used has been ethnography in two phases: one in locating the data controllers and the second sending subject access requests. The requests included questions related to personal data disclosure, the use of automatic making decision processes and data sharing with third parties. Strategies of facilitation and denial have been recorded, along with successful and unsuccessful cases.

Primary results show how compliance with the data protection law is the exception, especially in public institutions (even if the results show bad practice across the board). Often times, failure to comply with the law is also associated with more subtle denial and delay strategies aimed at discouraging the citizen from exercising his/her rights. In the end, the picture that emerges shows a landscape of unawareness of the legal framework, disregard for data protection and vulnerability.

Michel Foucault and the Smart City: Power and Surveillance Dynamics Inherent in Contemporary Governing through Code

Session: **PARALLEL SESSION 4** – City

Date and time: **25th April 2014. (09:15-10:45)**

Author: **Francisco Klauser**

Drawing upon Michel Foucault's approach to power and governmentality, the presentation explores the internal logics and dynamics of software-mediated techniques used to regulate and manage urban systems. My key questions are as follows: What power and regulatory dynamics do contemporary smart-city initiatives imply? And how do smart information technologies intervene in the governing of everyday life? Building on the Foucauldian distinction between 'apparatuses of discipline' and 'apparatuses of security', the presentation approaches these questions on three

broad levels, referring to how contemporary 'governing through code' relates to its referent object (referentiality axis), to normalisation (normativity axis) and to space (spatiality axis). Empirically, the paper investigates two high-profile pilot projects in Switzerland in the field of smart electricity management, aimed at (1) the assessment of customer needs and behaviours with regard to novel smart metering solutions (iSMART), and (2) the elaboration of novel IT solutions in the field of smart electricity grids for optimised load management (Flexlast).

Censorship

India: Evolving asymmetries in Surveillance

Session: **PARALLEL SESSION 4** – Censorship

Date and time: **25th April 2014. (09:15-10:45)**

Author: **Elonnai Hickok**

This paper will examine evolving shifts in surveillance practices and regime in India, and discuss how recent developments, such as the Central Monitoring System, perpetuate a deepening asymmetry of power created by poor implementation of existing safeguards, developments that exceed or bypass checks and balances currently in place, and a lack of transparency which removes surveillance from the purview of the public eye, thus preventing democratic debate and input into governmental surveillance.

In India, the asymmetry that arises is not limited to between the government and the people, but also extends to the intermediary. As intermediaries have become pivotal players in surveillance, they are subject to extensive and vague security requirements by the Indian Government, and are heavily penalized for non-compliance. This creates a situation where the service provider is presented with non-transparent requirements by the government, and little incentive to challenge extra legal requests for surveillance.

The asymmetries in power created by surveillance can be seen, and are perpetuated at many different levels including: 1.) In the imagination of a surveillance capability and regime – where the Indian government is shifting from surveillance capabilities that allow for re-active targeted surveillance, to that which will allow for pro-active mass and indiscriminate surveillance 2.) In the technical implementation of surveillance – where technological developments permit the creation and analysis of large data sets through many means including an expansion to platforms that allow harvesting of personal data and habits, thus permitting governmental surveillance platforms to be synthesized for large scale surveillance. 3.) In the legal regulation of surveillance – through a bypassing of traditional oversight mechanisms, and expansion of legal powers with regards to whom, how, and when legal surveillance can take place.

The paper will conclude that India is at a cross road, while considering a privacy legislation that could potentially regulate surveillance, and at the same time introducing projects that could impinge on the rights of its citizenry. The Indian Government is thus faced with broad questions about balancing contextual anxieties around national security and extra-territorial access, against the potential harm to the rights of the individual. At the same time, the Indian public is faced with

questions about the consequences of current and evolving surveillance practices, and about what balance needs to be struck to address the needs and nuances of the Indian society.

Freedom of Speech, Freedom of Association, Censorship and State Surveillance

Session: **PARALLEL SESSION 4** – Censorship

Date and time: **25th April 2014. (09:15-10:45)**

Author: **Andrew Adams**

The revelations by Edward Snowden of the activities of the US' NSA, the UK's GCHQ and other security services confirmed some of the worst fears of privacy activists previously considered cranks, now including evidence that the NSA has been intervening in the development of cryptography standards to keep them weak enough.

In recent years, other countries without the technical resources of the NSA had been (relatively) openly pressing communications providers to allow their intelligence services access to individuals' communications data. Blackberry were subject to this in Saudi Arabia, Pakistan and India , being required to make their email and instant messaging as accessible to interception as SMS. Blackberry were also the target of UK government pressure on use of their instant messaging service to coordinate rioters' activities in 2011. In 2011, the BART shut down cell-phone coverage entirely in areas subject to protests coordinated by mobile devices.

The Arab Spring, with unrest, changes of government or civil wars from Algeria to the Yemen, is often at least partially believed to be underpinned by new electronic communications from Twitter to Facebook to Skype.

Censorship runs from keyword-based limitations through dropping services and up to direct physical action against selected speakers. The goal of most governments at most times is not so much censorship as the encouragement of self-censorship. Without freedom of expression, freedom of association is much harder. If opposition to the current order is difficult or risky to express, then finding those with common cause and coordinating resistance activities becomes much more difficult.

This paper covers the socio-technical spectrum of surveillance, censorship and freedoms of speech and association as a key ideological battleground in the early 21st century.

The Lexicon of Fear: Chinese Internet-Control Practice in Sina Weibo Micro Blog Censorship

Session: **PARALLEL SESSION 4** – Censorship

Date and time: **25th April 2014. (09:15-10:45)**

Authors: **Juha Vuori and Lauri Paltemaa**

The paper analyses the 'sensitive word list' of the Chinese 'Sina Weibo' micro blog. The list has been generated by Sina Weibo users through crowdsourcing and contains over 1000 sensitive words. While Chinese Internet censorship has been extensively studied, thus far little attention has been directed to the actual word-level structure of Chinese censors' lexicon. In the paper, the lexicon is sorted out and analyzed quantitatively. It is argued that censorship mostly targets proper names of both natural persons and organizations, and only to a lesser degree phrases or abstract concepts such as 'democracy'. Censorship is also very contextual: it is as important who says what as what is being said. Moreover, censorship has flexible and stable parts. The on-average stay-time of most sensitive words is only a few months, yet censorship also contains the 'hard core' of semi-permanent sensitive words, which are not allowed in free popular discourse. Focaultian concepts of good, bad, and dangerous 'circulation' can be used to conceptualize such governance of words by security experts. aid the inhabitants of smart cities and smart homes in behaving sustainably, based on the assumption that behaviour can be changed using surveillance systems, coupled with a view of technology as a value-neutral vehicle for providing information to drive behavioural change. On the one hand, these systems allow human and non-human subjects to be governed at a distance by a central authority. On the other hand, they do not function according to their designers' intentions, and surveillance subjects exercise their own agency by resisting the watchful eye, or by shaping the technologies to suit their own needs. While recognising that climate change and environmental justice are, and will continue to be, significant concerns for contemporary societies, I question why surveillance is a highly prominent method in discourses of digital technological systems for sustainability. In conclusion, I suggest that the design and development of these systems stand to benefit from critical analyses by scholars in the field of surveillance studies, as these systems can potentially sustain unequal and unjust power relations, but they can also be effective tools for voicing social concerns.

Self-surveillance

Measuring our way to health

Session: **PARALLEL SESSION 5** – Self-surveillance

Date and time**: 25th April 2014. (11:00-12:30)**

Authors: **Pedro Sanches and Baki Cakici**

Recent advances in wireless sensor technology towards miniaturization and improved wearability have contributed to the growth of the field of commercial activity trackers, and led to the development of a wide range of applications in the intersections of wearable sensors and health. The term activity tracking describes a group of technologies that use wearable sensors to collect information about how individuals move. They convert the traces of the activities performed by the individuals to information about those activities in the form of calories spent, steps taken, distance covered, etc.

These technologies are not neutral. Rather than passively providing information, they act on individuals by constructing different types of embodiments and subjectivities in the name of health promotion. The discourse of the manufacturers promotes self-knowledge as a mean to achieve weight loss, health and happiness. Although some attention has been given to the possible implications of these technologies for embodiment and social relationships, little has been written about the subject's agency and appropriation of these technologies.

In this paper, we look at online posts related to activity tracking devices from a weight loss community. Users of these systems voluntarily subject themselves to a normalizing gaze, which converts their body activity to standard metrics. Through online profiles and community interfaces, these systems are designed to encourage their users to alter their behavior in the name of their health. But the nature of individual reactions to self-tracking systems is complex. We observe how the users' experience of self tracking ranges from accepting the systems metrics as the truth, to exerting their agency by co-constructing meaning of the bodily data generated by the sensors, contesting it and appropriating it. Documenting a range of experiences to activity tracking technologies from the users' point of view can be used to delineate more nuanced modes of compliance and resistance to self-tracking surveillance systems.

These networked self-tracking technologies and practices open up new questions relating to surveillance, privacy, ethics, and the self. Often, surveillance is understood as something externally imposed, controlling and disciplining (Norris and Armstrong, 1999; Foucault, 1977; Fuchs, 2008;

Gandy, 1993; Lyon, 2001), but this conception is challenged when individuals perform self-surveillance to collect quantified data for purposes of evaluation, management, optimization, and social interaction. Sharing collected personal data with peers online change the individual's reasonable expectation of privacy (Ess, 2009; Nissenbaum, 2010), and issues of ethical responsibilities regarding data ownership, commodification and sharing practices also become pertinent (Fuchs et al., 2011). Finally, the increasing documentation, quantification and broadcasting of the self change the dynamics of performing and producing subjectivity (Papacharissi, 2011; Vaz and Bruno, 2003; Warner, 2005).

The paper is guided by the following research questions: How does the translation of self into a quantifiable object produce subjectivity (as patient, athlete, learner, worker, etc.)? What role do potentially fragile technologies play in the mediation of the self? How do social interaction, entertainment, and gamification modulate the enactment of selfhood?

Self-surveillance: Quantification and tracking technologies

Session: **PARALLEL SESSION 5** – Self-surveillance

Date and time: **25th April 2014. (11:00-12:30)**

Author: **Anders Albrechtslund**

In this paper I explore, analyze and develop an understanding of self-surveillance practices. Gadgets and applications are increasingly being developed and used for tracking, quantifying, and documenting everyday life activities and especially health and fitness devices such as GPS-enabled sports watches are well-known and popular. However, self-surveillance practices involving networked technologies can be found across many domains, including culture, food, learning, work and general living. Individuals use tools and techniques to track themselves, thereby translating their own habits, bodies, moods, and thoughts into objects to scrutinize and transform. In addition, self-tracking is often coupled with social interaction and sometimes framed as entertainment or games.

These networked self-tracking technologies and practices open up new questions relating to surveillance, privacy, ethics, and the self. Often, surveillance is understood as something externally imposed, controlling and disciplining (Norris and Armstrong, 1999; Foucault, 1977; Fuchs, 2008; Gandy, 1993; Lyon, 2001), but this conception is challenged when individuals perform self-surveillance to collect quantified data for purposes of evaluation, management, optimization, and social interaction. Sharing collected personal data with peers online change the individual's

reasonable expectation of privacy (Ess, 2009; Nissenbaum, 2010), and issues of ethical responsibilities regarding data ownership, commodification and sharing practices also become pertinent (Fuchs et al., 2011). Finally, the increasing documentation, quantification and broadcasting of the self change the dynamics of performing and producing subjectivity (Papacharissi, 2011; Vaz and Bruno, 2003; Warner, 2005).

The paper is guided by the following research questions: How does the translation of self into a quantifiable object produce subjectivity (as patient, athlete, learner, worker, etc.)? What role do potentially fragile technologies play in the mediation of the self? How do social interaction, entertainment, and gamification modulate the enactment of selfhood?

Antidoping code and controls: Athletes' views and practices

Session: **PARALLEL SESSION 5** – Self-surveillance

Date and time: **25th April 2014. (11:00-12:30)**

Author: **Nils Zurawski**

Viewing doping controls in the lights of social sorting, puts a new perspective on the subject. Besides touching on issues such as data protection, citizens rights of informational self-determination, privacy and the right to be let alone, those controls foster forms of social sorting, albeit ones that claims to sort out particular subjects in the name of fairness. As much as doping practices are a problem to a culture of fairness and good sportsmanship, so are the controls.

From existing research, it is apparent that the athletes' perspective is missing in the discussion. The athletes are the object of the public debate, rather than the subject. Athletes that are convicted (or even only suspected) of doping practices are blamed and condemned – often by the same people that were generating the pressure under which the decision to take illegal performance enhancing substances was made. Doping and its controls therefore operate in a twofold field of social sorting: one that sorts out the guilty – and one that sorts out the losers, which may turn to illegal measures to improve their situation.

From interviews with athletes, officials and doping controllers on doping control practices, I will highlight what forms of social sorting are generated through doping controls, how they are perceived and what discourses are being formed.

I want to draw the attention to other issues within the debate on doping, such as have not received wide attention and are not likely to, as athletes more and more are put under a general suspicion within the system that is generating a massive pressure and puts athletes at risk. Social sorting is

by no means an intended consequence, but a „collateral“ effect that does play a major role on how these controls are perceived and hence legitimised.

States

Rethinking privacy to define surveillance

Session: **PARALLEL SESSION 6** – States

Date and time: **25th April 2014. (13:30-15:00)**

Author: **Rosa María García Sanz**

I will observe and analyse recent surveillance activities and identify the “new elements” and the consequences for citizens’ “private lives”. I will address the issue of whether security and freedom are more or less protected by the new “technology surveillance” used by the governments and private sector.

Our lives online are data, information and expression. Surveillance on the Internet is easier than ever. Every “key strike” provides a lot of meaningful data. Two fundamental rights are basic on the Internet: data protection and freedom of information and expression. These digital rights are the “trunk” from which other branches stem. The regulation and protection of these two rights are the initial protection for the others. A new understanding of “data protection” (privacy) is absolutely necessary in order to rethink “surveillance” in the public or private sector. The European law is too rigid and narrow, but the American perspective is too flexible and broad. We need to start again thinking about fundamental rights on the Internet in order to find a new way to provide security that maintains freedom.

This paper will focus on the public sector, i.e. government surveillance. Traditionally governance depends on surveillance in extreme circumstances to protect the rights and freedoms provided in the Constitution. We have a long tradition—and many reasons—to accept this kind of surveillance (to protect the country and citizens), but we cannot accept a government that acts as a “Big Brother” with expansive powers without limitation. A Big Brother enabled by “Big Data” can have the opposite result to the reason that traditionally legitimated the Government surveillance. Strong fundamental digital rights with strong protection online are the way to control the unlawful surveillance.

Exploring the relationship between procedural justice and surveillance studies: Experiences with surveillance during Canadian border crossings

Session: **PARALLEL SESSION 6** – States

Date and time: **25th April 2014. (13:30-15:00)**

Author: **Alana Saulnier**

Individual responses to surveillance span a continuum from willing compliance to active resistance (Ball, 2009). It is worth considering how and why personal reactions to surveillance fall differently on this continuum. This work couples procedural justice and surveillance studies literatures to develop our nebulous understandings of experiences with surveillance. Specifically, the theoretical model relies on the concepts of intersectionality, social sorting and cumulative disadvantage to hypothesize the ways in which experiences with surveillance during Canadian border crossings are stratified. Procedural justice theorizing offers an explanation of the effects of this stratification. Procedural justice is concerned with the extent to which a procedure (as opposed to an outcome) is perceived as fair and satisfactory (Tyler, 1989). Lind and Tyler (1988) maintain that procedures communicate symbolic messages of respect and value from the group to the individual. In particular, treatment by authorities during a procedure (in terms of respect, neutrality and standing), influences procedural justice evaluations because group membership is very important to individuals (Tyler, 1994). Encounters with surveillance during border crossings constitute a decision-making procedure in which permitted or denied mobility is the decision reached. The implications of procedural justice perceptions include that greater perceptions of procedural justice lead outcomes to be evaluated as more legitimate (Tyler, Degoey & Smith, 1996). Perceived legitimacy of authorities (or institutions) prompts an attitude of compliance with the future instructions of those authorities (Sunshine & Tyler, 2003) and engenders cooperative behaviours, even to unpopular decisions (Tyler & Degoey, 1995). In short, the extent to which persons perceive their experiences with surveillance as procedurally just is likely to wield considerable influence over evaluations of how appropriate or justifiable treatment during the encounter was and, therefore, the choice to invoke various strategies of negotiation or resistance. Implications for researching the experience of surveillance are discussed.

Double standards – an ethical questioning of different surveillance regimes for EU-members and third country nationals

Session: **PARALLEL SESSION 6** – States

Date and time**: 25th April 2014. (13:30-15:00)**

Author: **Elin Palm**

Recent advances in wireless sensor technology towards miniaturization and improved wearability have contributed to the growth of the field of commercial activity trackers, and led to the development of a wide range of applications in the intersections of wearable sensors and health. The term activity tracking describes a group of technologies that use wearable sensors to collect information about how individuals move. They convert the traces of the activities performed by the individuals to information about those activities in the form of calories spent, steps taken, distance covered, etc.

These technologies are not neutral. Rather than passively providing information, they act on individuals by constructing different types of embodiments and subjectivities in the name of health promotion. The discourse of the manufacturers promotes self-knowledge as a mean to achieve weight loss, health and happiness. Although some attention has been given to the possible implications of these technologies for embodiment and social relationships, little has been written about the subject's agency and appropriation of these technologies.

In this paper, we look at online posts related to activity tracking devices from a weight loss community. Users of these systems voluntarily subject themselves to a normalizing gaze, which converts their body activity to standard metrics. Through online profiles and community interfaces, these systems are designed to encourage their users to alter their behavior in the name of their health. But the nature of individual reactions to self-tracking systems is complex. We observe how the users' experience of self tracking ranges from accepting the systems metrics as the truth, to exerting their agency by co-constructing meaning of the bodily data generated by the sensors, contesting it and appropriating it. Documenting a range of experiences to activity tracking technologies from the users' point of view can be used to delineate more nuanced modes of compliance and resistance to self-tracking surveillance systems.

States and Governments

I surveil your citizens as you spy on mine: (Global) constitutional thoughts on the chiasmus in international IT surveillance

Session: **PARALLEL SESSION 7** – States & Governments

Date and time: **25th April 2014. (15:15-16:45)**

Authors: **Julian Staben & Hannfried Leisterer**

In the rise of the recent discussions about the PRISM programme of the US-American National Security Agency (NSA) the German Bundesnachrichtendienst's (BND, "Federal Intelligence Service") 100-Mio-IT-programme ("Technikaufwuchsprogramm") has come to light. Both programmes are focused on the surveillance of IT-based communication among foreigners and between citizens and foreigners. This fact has often been employed as a mitigating argument within the national legal and policy discussions. At the same time, both agencies conduct and widely rely on the exchange of intelligence information. This may in some cases amount to a factual circumvention of surveillance laws and basic constitutional rights. This paper examines some of the possible loopholes of national law. It reveals risks and damages that fundamental rights currently hardly protect against. Finally, possible solutions lying mainly in the field of global constitutionalism and public international law are assessed.

From supervision to electronic surveillance in the workplace, some ethical issues

Session: **PARALLEL SESSION 7** – States & Governments

Date and time: **25th April 2014. (15:15-16:45)**

Authors: **Anne Chartier, Marie-France Lebouc and Bernard Plante**

Surveillance in the workplace may take many forms from physical watching to automated tools. Availability and diversity of automated tools and their cheaper cost make them appealing to organizations. Doing so, there is a risk of a subtle shift from employees 'supervision' to employees 'surveillance' in the workplace. How do these two practices differ? What are the ethical issues linked to each of them?

The problems arising from the use of surveillance technologies and managerial practices relating to them are grounded in a philosophical questioning that pertains to ethics. Indeed, in order to design and select surveillance systems, managers and technicians picture employees in two different

ways. First, they have to label them as potentially deviant. Second, they need to segment them into attributes that will be translated into elements of surveillance and systems technical features. The shift from supervision to surveillance is an issue for fairness and employees 'respect' and it is one of justice.

The paper proposes a framework to analyse supervision and surveillance practices in the workplace as complex phenomenon involving three groups of actors: managers, information systems professionals and employees. In so doing, we put forth the ethical conditions of regulating behaviour taking into account elements of moral judgment Canadian philosopher Charles Taylor has identified, that is respect for the other, personal dignity, and meaningful life. Our framework goes beyond deliberation and includes elements such as emotions, cognitive bias and gut feeling. The proposed framework will help refine cognitive and moral determinants of the decision to implement surveillance systems in the workplace. It should contribute to enrich the theoretical understanding of the ethical issues of surveillance in the workplace.

The Coalescent State – Assemblages of public policy and governmentality in surveillance

Session: **PARALLEL SESSION 7** – States & Governments

Date and time: **25th April 2014. (15:15-16:45)**

Authors: **Chris Campbell and William Webster**

The paper examines the potential role of the assemblage as a fundamental critical tool within surveillance studies, and more widely in public policy and political science, by synthesising an approach between governmentality and policy analysis. The assemblage – a collection of things or 'pieces' of things within a single context – can bring about a number of effects, and while the surveillant assemblage has become an important touchstone in surveillance studies, this relationship between assemblant components and effects is critically underused. Assemblages attempt to territorialise themselves, by altering the constituent elements and 'mix' within the assemblage. These elements can be characterised in terms of expressive and material elements, which can then be traced through a time series of decision points, connecting both high level policy decisions and the subjectivity of the surveilled population. While public policy analysis tends towards rational models, this may be insufficient to deal with the complex modern policy environment, particularly with regards to surveillance, with its overlaps between privacy, safety, law enforcement practice, ethics, discrimination and structural violence. Similarly, governmentality offers limited practical tools for the policy-maker, tending to focus on the discursive constitution and

construction of government, with approaches that can lack a grounding in substantive practice or empirical reality. A synthesised approach to issues of policy is both robust and lends itself to empirical research. Such an approach provides a methodology and theoretical framework that can explain and map the existence (and persistence of) systems of power, increasingly important as surveillance practice becomes ever more asymmetrical. Public policy and surveillance systems are both best characterised as assemblages, on-going concerns that coalesce and crystallise around decision points. By providing critical insight that is agnostic as to the level of study, we can transform how we conceptualise policy and governance of surveillance in democracies. This transformed approach has important implications for the operation and management of both surveillant technologies and the democracy more generally.

Social Media

Techno-Security As Everyday Culture. On High-Tech Surveillance, Social Media and the Black Box of Technology

Session: **PARALLEL SESSION 7** – Social media

Date and time: **25th April 2014. (15:15-16:45)**

Author: **Jutta Weber**

Security today is increasingly reconfigured as maximum high-tech security relying widely on surveillance technologies. In parallel, surveillance technologies have become integrated in social media practices such as location sharing, profiling, or tagging. This paper aims at the development of the concept of "techno-security" (Mattelart 2010) culture starting from the premises that
- this culture is profoundly shaped by the impact of high-tech surveillance technologies and social media, their epistemologies and techno-imaginaries.
- today's preventive and extensive monitoring is not a disciplinary state activity alone but performed playfully in social media
- affective, normative and epistemological regimes inscribed into algorithms and databases drive our desires and configure contemporary techno-security culture.

In the following I will understand culture as a multifold, dynamic sociopolitical practice with a broad variety of agents and actants and as a heterogeneous, embodied and complex process in which not only states or other authorities but also software, concepts, machines, and humans participate in the production of meanings, standards, categories and norms. The techno-cultural approach takes the non-human actors of techno-security serious and scrutinizes how affects, categories and imaginaries are inscribed into software applications and databases.

In my paper I will explore how the framing of techno-security as culture would enable us to develop a broader understanding of how security governs policy and everyday life and especially how technology drives our desires and how desires drive our technology.

Location-Based Social Networks: GPS On, Privacy Off

Session: **PARALLEL SESSION 7** – Social media

Date and time: 25th April 2014. (15:15-16:45)

Authors: Renee Powers and Alessandro Panebianco

We have been leaving digital footprints through social networking since the very beginning. With

the ubiquity of social networks online, our "likes," tweets, and +1's record where we have been online. The popularity of smartphones and GPS technology has enabled social networks to hybridize into offline spaces as well. Not only can a user "like" her favorite bakery on Facebook, she can also "check-in" to notify her friends in real time that she is visiting the bakery. Apps like Foursquare and Gowalla have popularized these check-ins via location-based social networks. Many users are rewarded with company perks like free appetizers or discounts when they check in regularly to a location. Yet even more traditional social networks like Twitter and Facebook have begun incorporating users' physical location. Facebook users now have the option to check-in to locations, much like Foursquare. Our concern is how users conceptualize privacy in this hybridized digital-physical space. We collected survey information about location-based social networking application users' privacy behaviors and recruited three volunteers from this sample. Using only the volunteers' public location-based or geotagged social networking information, we developed profiles that we presented to them in individual interviews. The volunteers were not especially surprised to see how much and what kinds of information we collected but had surprising comments about their own strategies for privacy maintenance.

Will your Facebook profile get you hired? Employers use of information seeking online during the recruitment process

Session: **PARALLEL SESSION 7** – Social media

Date and time: **25th April 2014. (15:15-16:45)**

Authors: **Hedenus Anna and Christel Backman**

Over the past years it has become increasingly more common for employers to check up job-seekers online, using a search engine, specific databases or social media. In this way employers may add information about specific parts of the job-seeker's past, such as criminal records, or try to capture the job-seeker's "data double". Previous research on online behaviour in general and social media in particular, has focused on the data subjects online action, how privacy settings are used and if online behaviour is modified depending on potential data gathering by outsiders. In this paper we turn our attention to the ones who gather this type of data and use it as access control for employment. Our aim is to examine how employers interpret the data they find and to what extent it influences the recruitment process and the decision to hire or not hire a candidate. We present findings from a pilot study consisting of ten qualitative interviews with employers who use search engines to find additional data on job-seekers. In the paper we discuss the different ways in which information gathering on Internet is used, how it affects the recruitment process, how employers

relate the “data double” to the identity presented by the job-seeker, and how ethical dilemmas are handled by the employers. We also discuss the ethical implementations of moving data from one context to another were it may be interpreted according to different norms, and show how this form of surveillance can be either beneficial or discriminatory for the subject depending on the information found and what the employer perceive as important aspects for the organisation.

Social Media: policing, profiling

Social Media Policing and Intelligence: A European Approach

Session: **PARALLEL SESSION 8** – Social media: policing, profiling

Date and time: **25th April 2014. (17:00-18:30)**

Author: **Daniel Trottier**

Police and other law enforcement agencies face new challenges and opportunities with the emergence of social media platforms. Not only are these sites a potential jurisdiction to monitor, but they are also a potential source of evidence for other crimes. As a result, investigative agencies and private companies have developed several categories of technologies that monitor social media, and analyse their content. These technologies are being trialled in a global context, and EU member states in particular are contemplating the extent to which police practice should adapt to these investigative technologies.

After briefly outlining the range of social media monitoring technologies currently available, this paper considers issues surrounding online evidence and intelligence collection. It draws upon interviews with nineteen police representatives and fourteen privacy advocates from thirteen EU member states. Findings are arranged along the following key dilemmas: Should investigative agencies adopt these techniques and technologies? If they do, what are the social, cultural, political, practical and legal justifications for doing so? How will these efforts be financed? What kind of training will be necessary? What kind of human effort is required in social media monitoring, and to what extent can these tasks be – and should be – automated? To what extent are social media monitoring technologies interoperable with other kinds of data collection?

Social Media Profiling: a Panopticon or Omniopticon Tool?

Session: **PARALLEL SESSION 8** – Social media: policing, profiling

Date and time: **25th April 2014. (17:00-18:30)**

Authors: **Miltiadis Kandias, Lilian Mitrou and Dimitris Gritzalis**

Online Social Networks and Media indicate and incorporate the shift to interpersonal, horizontal, and mutual communication and, consequently, information aggregation. Online content (namely YouTube videos and comments or Tweets) along with online relations (friendships, followings, mentions, comments etc.) may be crawled and utilized for a variety of purposes including user/usage profiling and behaviour prediction. In our previous research we have proven that it is

possible and even potentially trivial (by utilizing a simple personal computer and a broadband internet connection) to extract sensitive, personal information such as political beliefs, psychosocial characteristics (narcissism and predisposition towards law enforcement) etc. about social media users in an automated manner via data crawling, data aggregation, machine learning and graph and content analysis of the collected dataset of YouTube and Twitter Open Source INTelligence. Web 2.0 technological features combined with voluntary exposure to an indefinite audience in social media give rise to traditional surveillance as Government is enabled to "connect the dots", combine information about political beliefs and every-day activities and generate mass user profiles on the base of identifying patterns. Despite the lack of centralized control over the Internet, its platforms and applications allow multilevel and latent surveillance, thus pose new risks for individuals by forming new power relations and asymmetries. Our research highlights how Web 2.0 and social media (YouTube and Twitter) may become a topos of "participatory panopticism", an Omniopticon, in which "the many watch the many" and can reconstruct sensitive information out of seemingly anonymous data/content. Individuals may be confronted with social exclusion, prejudice and discrimination risks both in their workplace and in their social environment. In our paper we focus on the results of this type of surveillance which facilitates the exculpation of such penetrating and privacy-violating technologies and amplifies the threshold of societal tolerance towards a panopticon-like state of surveillance.

Is Policing Surveillance of Online Social Media Out of Control? : A UK Legal Perspective

Session: **PARALLEL SESSION 8** – Social media: policing, profiling

Date and time: **25th April 2014. (17:00-18:30)**

Authors: **Lilian Edwards and Lachlan Urquhart**

This paper will argue that law enforcement agency (LEA) surveillance of online social media is becoming commonplace, without parallel development of adequate legal structures to protect civil liberties. Online users routinely share copious amounts of personal data, including intimate detail about their daily activities, thoughts and experiences, on social networking platforms; consequently these are known to have become a valuable intelligence resource for LEAs. High profile events, such as the London riots in summer 2011, as well as the revelations concerning, first, US intelligence use of Raytheon Riot software in 2012, and then the extensive backdoor NSA access to social media data in both the US and UK revealed by Edward Snowden in 2013, have made this a source of major public concern. Users of social media have arguably created a near-perfect

panopticon, in Foucault's terminology, for unobserved and uncontrolled mass surveillance of themselves. Worse still, the keepers of the panopticon are not a state authority accountable to public scrutiny but commercial bodies who owe minimal obligations of accountability and transparency.

The paper will focus on UK legal regulation, and compare curbs on traditional non-digital direct and covert surveillance by police to those on surveillance of social media and digital communications, and then ask whether existing regulation is adequate to protect values including privacy, autonomy and due process. Relevant UK and EU laws will be analysed, including, notably, the Regulation of Investigatory Powers Act 2000 (RIPA) and we will conclude that UK law presents few bars to general social media surveillance eg by topic or hashtag, and even targeted social media surveillance of individual profiles remains a grey area.

School

RFID as a surveillance technology: A Comparison of RFID and CCTV Through a Content Analysis of Media Discourse surrounding the Introduction of RFID in the Northside Independent School District

Session: **PARALLEL SESSION 7** – School

Date and time: **25th April 2014. (15:15-16:45)**

Author: **David Neumann**

Radio Frequency Identification (RFID) has been widely used in the past 15 years mainly to track cattle and inventory. Up until recently, little to no scholarship had been found on the media discourse surrounding the use of RFID to track humans. Enter the Northside Independent School District in Texas which recently implemented a pilot program that would track students for attendance management. While this school was not the first to implement RFID to track students, due to the complaints of one student (Andrea Hernandez), the program gained international attention. In order to give the media discourse surrounding the Northside program some context, a comparative content analysis of the media discourse surrounding close circuit television (CCTV) surveillance was compared to the media discourse surrounding the Northside project. CCTV was selected as a comparison with RFID because it is the predominant surveillance technology that has studies and scholarship written about it. Thirteen articles were therefore analyzed for key themes and expert voices and were compared against a similar study done on the general media discourse surrounding CCTV surveillance. While RFID technology for humans may still be in an "embryonic state", the media discourse themes, and "primary definers" are well established which should worry those who oppose these types of surveillance technologies for humans.

"The mark of the beast"? Reverence and resistance to RFID in schools

Session: **PARALLEL SESSION 7** – School

Date and time: **25th April 2014. (15:15-16:4**5)

Author: **Emmeline Taylor**

Analysed within the context of the Surveillance School, this paper explores the use of RFID in schools from a comparative perspective. Whilst RFID has been trialled in schools in places such as the UK, the Philippines and South America, it is Japan and some states in the US that are leading the way in the RFID tracking of pupils. RFID microchips are commonly embedded in school passes

which are required to be carried or worn at all times by pupils, whereas some schools embed the chips into 'smart uniforms' or use conductive 'smart threads' embroidered onto school jumpers. The objectives of RFID are diverse and although safety is often presumed to be the impetus a cursory look at the myriad objectives belies this. Borrowing library books, claiming revenue for attendance, purchasing lunch; RFID has found many applications. This paper focuses on the reverence that some countries have demonstrated for this technology and outlines the reasons why others have resolutely resisted RFID in the school context. The paper concludes with a consideration of how resistance to everyday surveillance manifests and to what extent it can change surveillance systems.

An Evaluation of Winnipeg's Electronic Monitoring Program for Youth Auto Theft Offenders

Session: **PARALLEL SESSION 7** – School

Date and time: **25th April 2014. (15:15-16:45)**

Authors: **Ashley Pearson, Rick Linden and Denis Bracken**

Electronic monitoring of offenders has had limited use in Canada covering a relatively small group of offenders in 7 of the 13 provinces and territories and at the Federal level. The focus of this paper will be to examine an EM program implemented in 2008, by the province of Manitoba for high-risk youth auto theft offenders. This program was evaluated using a combined methods approach, a qualitative and quantitative analysis. The evaluation included one to one matching of the youth on EM to other high risk auto theft offenders who had not been on EM as well as interviews with probation officers, offenders, and other stakeholders. Quantitative analysis revealed small changes in criminal history for the EM group for auto theft, technical and combined offences. Qualitative results suggest that EM provided probation officers with useful information with respect to curfew compliance and resulted in some cases in increased intervention, but it was also perceived as limiting their discretion in some areas. Although there has been a decrease of approximately 11,000 auto thefts over the past 9 years (beginning before the EM program was initiated) the results of this study suggests only a very small part of this decrease could be attributed to the EM program. However, we suggest that Electronic Monitoring as an intervention can be a complimentary program when offered in accompaniment with other program designed to reduce young offender auto thefts.

School and youth

Lateral Surveillance in Singapore

Session: **PARALLEL SESSION 8** – Schools and youth

Date and time: **25th April 2014. (17:00-18:30)**

Authors: **Hee Jhee Jiow and Sofia Morales**

With the high Internet penetration rate, and the dense saturation of audio-visual-capturing mobile smartphones among its citizens, Singapore provides a ripe technological infrastructure for a surveillance society. Its citizens have been serendipitously capturing, on photo or video, socially undesirable and controversial incidents of daily living. Widespread adoption and use of social media have enhanced the viewership of these behaviours captured, and provided a platform for responses of criticisms.

Panopticism, in the modern day context, is used as a metaphor to describe the effect of surveillance by authorities that shapes and manipulates social behaviour. Lateral surveillance is an opposite of panopticism, which portrays the impact of surveillance of the few, by the unseen many. This study explored the perception and impact of these activities on citizens' social behaviours. Respondents were questioned on their awareness of surveillance in different milieu of their daily lives, such as commuting, driving, interactions in public spaces, and checking into, or uploading of photos onto social media, and its impacts on their social behaviours in those public spaces. This study recruited a sample of 223 university students, aged between 19 and 24 years, comprising of both genders, to undergo an online survey. These students were directed to an online survey, which did not capture identifiable information, by the authors who have access to the students at their university.

Data collected provided descriptive statistics of the awareness and impact of panopticism, and lateral surveillance, by media-rich and media-savvy young citizens. Comparisons were made between panopticism versus lateral surveillance's effect on social behavior. This study found that lateral surveillance had a more powerful effect on social behaviours, contributed significantly by the presence and usage of publicity channels such as FaceBook, and other local popular news websites.

Living in the Mirror: Understanding Young Women's Experiences with Online Social Networking

Session: **PARALLEL SESSION 8** – Schools and youth

Date and time: **25th April 2014. (17:00-18:30)**

Authors: **Valerie Steeves and Jane Bailey**

Our paper presents the findings of a qualitative study that explored girls' lived experiences of watching and being watched online. Our participants' reading of markers like makeup, clothing and boyfriends to signal femininity online demonstrates their facility with the heteronormative ideal, as does their ready acknowledgement of the link between the sexualisation of this pretty, thin feminine body and social power (Hellman, 2008). In this sense, the online world duplicates the offline world (Van Doorn, van Zoonen and Wyatt, 2007), as girls are required to negotiate with the "untroubled" status (Hauge,2009) of the type of body assumed to be most privileged by the male gaze. However, our findings suggest that social media not only replicate the centrality of this binary classification (Manago, Graham, Greenfield, Salimkhan, 2008), they amplify it, in three inter-related ways. First, commercial surveillance intensifies girls' interactions with media representations and restructures the environment in ways that privilege heteronormative performances of girl. Second, the surveillance of family members and peers creates a gendered burden to care for and manage others' expectations; managing this burden is complicated by the ways in which that same surveillance breaks down the boundaries between performances of various identities, particularly because the demands of mainstream performances conflict with other identities they inhabit. Third, the visual nature of social media alienates the feminine body through the hyper-visibility of the image of the body; this makes the body an object of judgment that is subject to scrutiny by others and the self, and exacerbates the negative effects of failed performances. Our results suggest that an account of surveillance that incorporates panoptic, synoptic and interpersonal forms of watching offers greater potential for better understanding the surveillant forces that tend to undermine the potential for digital media to rupture the male gaze theorized by Mulvey (1975).

The shift in the role of the teacher in contemporary school: from the intellectual to the servant

Session: **PARALLEL SESSION 8** – Schools and youth

Date and time: **25th April 2014. (17:00-18:30)**

Authors: **Ott Puumeister and Mirjam Puumeister**

We are interested in the (shifting) power relations in the school environment. We start with the hypothesis that, in addition to the continuous development of surveillance techniques and technologies, there has been an emergence of technologies that make possible practices of sousveillance (mostly, of course, smartphones). Considering this, the school can no longer be unambiguously seen as a panoptic institution (which does not mean that it still would not incorporate important elements from this „diagram of a mechanism of power"). However, we do not argue that sousveillance technologies would inherently be directed at the teachers or the administrators of school. The behavior of other students will also be under close scrutiny, and in this way, sousveillance can also be seen as one element of expanding surveillance techniques. Taking as our examples cases from Estonian school environment (which is a quite typical example of a neo-liberal school), we wish to examine the power relations that are revealed in sousveillance practice. Most importantly, we will problematize the notion of the teacher as servant, the one who „tends to the customers" needs. The neo-liberal view of education has made the teacher serve both the student and the state or the market, thus transforming the figure of the teacher from an authority figure and an intellectual to a public servant. This transformation has, of course, significant consequences on the possibilities of educational environment.

The 'named person': surveillance and the wellbeing of children and young people in Scotland

Session: **PARALLEL SESSION 8** – Schools and youth

Date and time: **25th April 2014. (17:00-18:30)**

Author: **Eric Stoddart**

The Scottish Government (Scottish Nationalist Party) has placed a Bill before the Holyrood Parliament that seeks to legislate the administration's aspirations that public bodies do all that is necessary to ensure the wellbeing of every child in Scotland. This paper focuses on one element, the 'named person' that the Children and Young People Bill (Scotland), 2013 proposes as an identifiable professional within the healthcare or education systems who will be more than a point of

contact.

The role envisaged for the 'named person' is the subject of significant criticism, not least from the Faculty of Advocates (the body of independent lawyers admitted to practice as Advocates before the Courts of Scotland). Whilst many charities are supportive, the Faculty identifies a threat to traditional parenting responsibilities and freedom.

The criticisms directed at a similar Westminster initiative by the previous Labour government are seemingly ignored in the face of current moral panics that 'something must be done for vulnerable children.'

The 'named person' is defended by its supporters as a proportional response but this paper argues that the extension of surveillance implicit (and explicit) in the Bill is not adequately articulated. Whilst public debate still tends to lean on the 'Big Brother' analogy, an analysis drawing upon more adequate models of surveillance as social sorting is required. The notion of (in)visibility – negotiating one's visibility in social space – is further deployed as a critical device.

The Parliament's Education and Culture Committee is currently scrutinizing the Bill. Through a close reading of the evidence presented to the Committee and its questioning of witnesses, this paper exposes the threat to liberty that an attenuated understanding of surveillance poses when otherwise well-meaning legislation is proposed.

Policy/penal monitoring

Negotiating electronic surveillance

Session: **PARALLEL SESSION 8** – Policy/penal monitoring

Date and time: **25th April 2014. (17:00-18:30)**

Authors: **Johann Chaulet and Camille Allaria**

Our paper is based on two field studies. The first one deals with the surveillance of workers in call centers; through ethnographic observations, we have been analyzing the work of employees and their controllers. The second one deals with prisoners' electronic tagging and the work of judges and prison workers. Our communication will document, from a sociological point of view, the way ICTs are used to monitor activities and control bodies and how they can also be used in return to escape surveillance. Comparison will be detailed through different concepts such as ICT mediated surveillance, equipped conformity statements, contractual frame or criticism. We will focus on specific moments of negotiation. First of all we will address the way conformity itself is discussed; we will see how rules and procedures can never be precise enough to answer to every situation controllers may have to define and judge. We will examine the uses made of clues offered by surveillance tools, how they are mixed together in a personal way corresponding to specific conception of what is right or wrong, legitimate or illegitimate. This will lead us to present the strategies developed to escape or discuss surveillance, negotiating both with the devices and the controllers from a technical and social point of view. In the end, taking advantage of the common points and differences between the situations we will analyze, we will discuss the aim of these forms of negotiation, their social impacts and roles, on social order or everyday critical activities.

Between convict and ward: The experiences of people living with offenders subject to electronic monitoring

Session: **PARALLEL SESSION 8** – Policy/penal monitoring

Date and time: **25th April 2014. (17:00-18:30)**

Author: **Delphine Vanhaelemeesch**

Electronic monitoring does not only affect offenders who are monitored but also impacts on the life and position of those who share their lives with these offenders. Since policymakers and research only pay little attention to co-residents a qualitative research project was developed to study their feelings, understandings and impressions. The paper analyzes the experience of 30 co-residents of

offenders who are being electronically monitored in Belgium. It finds that they see their position balancing between two very different and even competing roles: a “convict” and a “controller”. On the one hand, co-residents report changes in their daily and social life that make them feel as if they are being punished themselves. On the other hand, they see themselves as active in the administration of the punishment and become assistants, social workers and controllers of the electronic monitoring sanction and take up roles as private individuals that were previously fulfilled by government. Co-residents are heavily involved in electronic monitoring and their experiences point to new forms of carrying out sentences in which the state further spreads and diffuses the application of its power.

What does electronic surveillance mean? A socio-historical account of the emergence and diffusion of electronic tagging of offenders

Session: **PARALLEL SESSION 8** – Policy/penal monitoring

Date and time: **25th April 2014. (17:00-18:30)**

Author: **Anna Vitores**

This paper shows, through the example of the emergence and diffusion of electronic tagging of offenders, that neither technological determinism nor social determinism is able to make the complex relationships between surveillance technologies and society intelligible. Among the wide literature on electronic tagging dealing with its sociological and practical implications, one can find that, once again, a political argument has arisen about the responsibility of technology in societal change. Some argue that electronic monitoring is only an instrument, that is, it could only imply a risk if misused. Others argue that this position entails the fallacy of technical neutrality, and that technologies have politics. Moreover, debates surrounding electronic tagging reproduce both indulgent and dystopian interpretations of the proliferation of surveillance devices. Departing from the problematization of the idea of “social impact” carried out from science and technology studies (STS), I want to offer a specific account of the emergence of electronic tagging drawing attention to the discontinuities and ruptures in those practices associated with monitoring offenders from its origin. According to this account, the practice of tagging is not defined only by technical properties, by dominant conceptions of managing crime or by specific notions of the individual. Rather, it is an effect of specific arrangements between all these heterogeneous components. An arrangement that is certainly irreducible to the explicit intentions of human actors or to the inherent features of techniques but nevertheless evidencing an orientation toward a particular matrix of ends. Furthermore, addressing some of the characteristics of electronic monitoring through its nature,

sense, uses and effects, subjects and function along time, it is possibly to identify different practices tied to the use of tags with prisoners and also different regimes of surveillance and power linked to those practices.

Biometrics

The Curious Case of the use of Biometric Reporting Kiosks in the UK Probation Service - Robohero or Roboflop?

Session: **PARALLEL SESSION 9** – Biometrics

Date and time: **26th April 2014. (09:15-10:45)**

Author: **David Raho**

Probation Officers in the United Kingdom have always valued the face-to-face supervisory relationship they have with their clients as the primary vehicle for bringing about rehabilitative changes rather than relying on electronic monitoring and other more potentially punitive control measures despite political pressure. Many of the more recent developments in rehabilitation, such as desistance approaches, depend on probation officers engaging with their clients effectively and getting to know them holistically and emphasise the importance of developing authentic professional relationships based on an understanding of a clients individual complex needs and motivation to change.

The introduction of biometric reporting kiosks threatens to bring about what Bauman (1995) has described as 'bureaucratically promoted adiaphorization'. In a probation context, it is argued, that this not only produces distance between the client being supervised (the survielled) and the probation officer (the surveillant other) but that it fundamentally alters the relationship between the client and the probation officer by adding a layer of technology that replaces professional human to human interaction and reduces and dehumanises the supervisory relationship to the level of a mechanised transaction.

The ordinarily 'moral' relationship between client and probation officer is then carried out via the medium of the kiosk this can be described as a stripped-down version or simulation of a relationship, lacking in aspects of the human, and not spatially and temporally whole, therefore it might be described as being an 'immoral' process as it no longer involves direct responsibility between humans but rather a partial artificially simulated relationship mediated through the kiosk.

It is therefore argued that the perceived potential benefits of biometric kiosk reporting are far outweighed by the costs associated with the loss of 1:1 human interaction with trained professionals.

Biometrics in beta: experimenting on a nation (while normalising surveillance for 1.2 billion people)

Session: **PARALLEL SESSION 9** – Biometrics

Date and time: **26th April 2014. (09:15-10:45)**

Author: **Malavika Jayaram**

In the developing world, privacy is often portrayed as a luxury, as something alien to local culture and of interest only to the elite. This ignores the probability of the most marginalized sections of a society being disproportionately impacted by privacy intrusive technologies. The hype about 'big data', 'open data', 'data for development', 'ICT4D' and other buzzwords often ignores the fact that the global south is particularly vulnerable to data collection and processing. Literacy issues (lingual and technical), a massive digital divide, desperate socioeconomic conditions and the lack of a robust data protection law render ideas of consent or tradeoffs all but meaningless.

Techno-utopian welfare schemes present technology as progressive, neutral and frictionless – a seductive and compelling narrative in a region wracked by inequalities, corruption, lack of transparency and structural violence. This vision underpins the world's largest biometric ID project, which has already registered the irises and fingerprints of 540 million people without even being completed. Yet the assumption that bodies can be rendered into infallible verifiers, as repositories of unchanging truth, ignores embedded biases and normative baselines within such technologies. Welfare projects are further complicated when they are architected as public-private partnerships: the collusion of governmental and corporate agendas in creating massive databases and profiles, in a manner that transforms the citizen-state relationship in profound ways, has sweeping implications for choice, autonomy, anonymity and ultimately, democracy. This is true even when the systems function as intended, without mechanical failure, data breaches, or other consequences of trading privacy for convenience, welfare and security.

I would like to discuss the risks of using technologies such as biometrics to solve socioeconomic problems, and their potential for excluding the very demographics that they seek to include. I intend to locate my presentation in the context of India's growing surveillance state, which deliberately intends to use the unique identification number to link disparate databases. I propose to describe the new Centralised Monitoring System, the relative legal vacuum in which data is mined and harvested, and the shaky constitutional foundations on which many of these new regimes stand. In so doing, I will effectively have provided a tour of India's Rogue's Gallery of recent incursions into the zone of privacy, free speech, informational self-determination and dignity. I hope also to redress in some small measure the largely western focus of academic and policy debates in this field,

despite the risks of developing countries seeking to commoditize and export identity schemes, normalize censorship or opportunistically benefit from the west no longer having the moral ground to resist third country surveillance practices.

New Surveillance Technologies & Their Publics: A Case of Biometrics

Session: **PARALLEL SESSION 9** – Biometrics

Date and time: **26th April 2014. (09:15-10:45)**

Authors: **Aaron K. Martin and Kevin Donovan**

Before a newly-elected government abandoned the project in 2010, for at least 8 years the British state actively sought to introduce a mandatory national identification scheme for which the science and technology of biometrics was central. Throughout the effort, representatives of the government attempted to demonstrate biometrics as a technology that was easily understandable and readily accepted by the public. However, neither task was straightforward and, instead, particular publics emerged that showed biometric technology was rarely well-understood and often disagreeable. Indeed, in contrast to some traditional conceptualizations of the relationship between public understanding and science, it was often those entities that best understood the technology that found it least acceptable, rather than those populations that lacked knowledge. This paper analyzes the discourses that pervaded the case in order to untangle how various publics are formed and exhibit differing, conflicting understandings of a novel technology.

UAVs/ Drones

The Surveillant Eye in the Sky: A Preliminary Investigation and Mapping of Unmanned Aerial Vehicles (UAVs) as a New Technology of Surveillance (in Canada)

Session: **PARALLEL SESSION 9** – UAVs / Drones

Date and time: **26th April 2014. (09:15-10:45)**

Author: **Ciara Bracken-Roche**

The applications for unmanned aerial vehicles (UAVs) are expanding in Canada, and internationally. Recent surveys conducted on privacy show that Canadians are not comfortable with UAVs for the use of public monitoring (Phoenix 2013). However, most Canadians are comfortable with the use of drones for search and rescue missions, border patrol, and law enforcement patrols (Ibid.). The shifting application of UAVs from the military to the civil context (Van Veeren 2013) warrants further research. Building on what is known about other forms of visual surveillance, notably terrestrial camera surveillance, the paper will explore what changes when aeriality and increased mobility are added, as in the case of UAVs. Traditional forms of visual surveillance that are fixed and grounded are frequently visible to those under surveillance; this contrasts with UAV surveillance that is highly mobile and far more inconspicuous (Lyon 2013). Sanctioned uses of UAVs include policing, law-enforcement and public order functions, but general issues of privacy and data protection are still highly relevant (Martell 2013; Wolf 2012; Wall and Monahan 2011; Walters and Weber 2010). Some questions that will be touched upon with regard to the deployment of these systems are: how does the use of unpiloted systems in civil applications impact upon privacy and other civil liberties? How does the use of technological systems of remote surveillance engage with the corporeal politics of space, place and identity? What are the social and political implications of these enhanced technologies of surveillance? Do they constitute mobile sites of pre-emptive risk assessment and identity management (Wall and Monahan 2011)? Through an analysis and tracking of UAV operations in Canada over the past 10 years, this work aims to start addressing these questions. UAVs are not entirely distinct from other types of surveillance but they are significant in that they raise new challenges due to their layered surveillance capabilities. Issues of behaviour monitoring, effects on democratic participation, function creep, and privacy all need to be considered with relation to these new systems of surveillance.

Tracing the Rise of UAVs in Canada

Session: **PARALLEL SESSION 9** – UAVs / Drones

Date and time: **26th April 2014. (09:15-10:45)**

Author: **Adam Molnar**

Unmanned Aerial Vehicles (UAVs), commonly known as drones, are being rapidly introduced in a range of public and private industries. In the US, the Federal Aviation Authority estimates that as many as 30,000 UAVs will be flying domestically by 2020 (Thompson 2013). These vehicles are, and will be, used for military, commercial, and law enforcement purposes. High adoption of UAVs is significantly driven by the large number of technical systems that can be 'attached' to the vehicles for surveillance, and combat interdiction functions. In civilian applications especially, UAVs are increasingly valuable for authorities' use in public safety, law enforcement, border patrol, and emergency services (Thompson 2013; Finn and Wright 2012). UAVs are 'changing the game' for intelligence gathering, data processing, and communications systems used by government forces and authorities. Given the capacity for these vehicles to enhance and modify state power in novel ways, it is critical to examine the socio-technical systems, policy development, and related political implications associated with UAV deployment in domestic jurisdictions.

Current research predominantly focuses on US-centric military operations, and to a lesser extent, domestic US applications of UAVs (Vogel 2010; Finn and Wright 2012). However, far less is known about how Canadian government institutions are using UAVs, both in terms of the justifications and applications for UAV deployment, and the convergence(s) between foreign military applications and domestic authorities' uses. Drawing on interviews with law enforcement officials, as well as government documents acquired through Access to Information and Privacy (ATIP) legislation, this paper interrogates how Canadian authorities are adopting UAVs for domestic purposes—and whether, or not, this involves a wider drift towards the militarization of domestic authorities in Canada.

Surveillance in the Drone Age: A Cyberconstitutional Moment?

Session: **PARALLEL SESSION 9** – UAVs / Drones

Date and time: **26th April 2014. (09:15-10:45)**

Author: **Philip Boucher**

Drones are most often associated with military surveillance and combat operations but several potential non-military applications have also been identified. Europe and the USA are in the

process of integrating these drones in their normal airspace. Among clearly beneficial uses such as search and rescue, they also offer the potential for enhanced surveillance. They are small and quiet enough to fly unnoticed and also cheap and independent enough to run persistently. They can be modified with cameras, heat sensors, motion detectors and microphones of a similarly surveillance-friendly specification. They may be used (legally or illegally) by police, corporations and individual citizens as well as spies, criminals and terrorists.

The USA's airspace integration plans were delayed in 2012 due to concerns about excessive surveillance raised by public commentators. The EC's integration roadmap (2013) recognised these concerns but suggested that existing laws offer sufficient protection. Both the USA and EC maintain that airspace integration will be achieved, by 2015 and 2016 respectively, and expect rapid development by state and commercial actors thereafter. How can the EC ensure its roadmap does not lead to the normalisation of technological activities that conflict with its citizens' rights and values? What can it learn from the delays experienced in the USA's strategy? What are the opportunities for citizen empowerment?

We explore these questions through a comparative analysis of consultation processes and integration strategies. Interesting features of the study include the taboo of the word 'drones', the strategic disassociation of military and non-military applications and the transatlantic differences in the relationship between citizens and the state (including legal and societal conceptualisations of privacy). Finally, following Jasanoff's concept of bioconstitutionalism, we consider the extent to which drone integration can be seen as a cyberconstitutional moment in which the relationships between human beings, technologies and the state are transformed.

Investigations

Security and privacy: Toward balanced risk awareness

Session: **PARALLEL SESSION 9** – Investigations

Date and time: **26th April 2014. (09:15-10:45)**

Author: **Regina Berglez**

The presentation will summarize the work done in WP3 “Exploring the Challenges”. Key concepts of security and threat are discussed and the issues of using technological solutions to handle these threats are highlighted. Investments in surveillance-based security technology are justified with the need to counter existing or emerging security threats. Relating a variety of discourses (legal theory, technology assessment and social sciences), the effects of these technological solutions on privacy rights can be assessed from a different angle. WP3’s legal dimension offers an analytical alternative, namely the “core/periphery approach”, which is based on the inviolability of the essence of any fundamental right. A technology assessment perspective explores possibilities and constraints of lawful and ethical deployment of security-related technologies (i.e. privacy by design). From a social science perspective non-technical solutions to security problems can be identified, and investigated in their ability to serve as alternatives to technology-centred solutions. Potentialities and limitations of societal-based concepts and approaches are presented and discussed.

An assessment of the desired security enhancement as well as the impact on human rights is needed to balance the use of technologies against the principles and ideals of a democratic Europe respecting the fundamental rights of its citizens. A holistic approach to societal, legal and technological solutions can lead to “balanced risk awareness”, perceiving security and privacy in a comprehensive way.

We state that living in late modern societies requires (1) a shared understanding of acceptable and desirable levels of consumer convenience, (2) an informed debate about an appropriate degree of citizen involvement, which needs to be accompanied by (3) an informed public debate about “acceptable” risks, taking into account that (4) fundamental rights such as the right to privacy should not be abandoned for an illusion of security.

Criminal investigation through the eye of the detective: technological innovation and tradition

Session: **PARALLEL SESSION 9** – Investigations

Date and time: **26th April 2014. (09:15-10:45)**

Authors: **Diana Miranda and Helena Machado**

The traditional image of the detective and the nature of police work is being transformed by the impact of technological elements and scientific knowledge. Despite the potential use of science and technology on criminal investigation, there are obstacles questioning its application. In order to explore these obstacles and using a qualitative and comprehensive methodology based on a set of semi-structured interviews with criminal investigators, we analyse their views concerning practices of identification and surveillance aimed at crime suspects and convicted offenders. Through theoretical contributions from social studies of science and technology, surveillance studies and policing we will analyse how soft and hard forms of surveillance are applied in the practices of Portuguese Criminal Investigation Police (Polícia Judiciária). The technological artefacts shape and are shaped by criminal investigators and it is necessary to explore how the collectives of human and non-human elements are constituted. Analyzing the conjugation of traditional methods of criminal investigation (hard surveillance) with new technologies of collection and use of information (soft surveillance), a hybrid figure of detective emerges as a creation of two times: past and present.

In a context where innovation sometimes is not possible, traditional methods endure. Nevertheless, the expansion of computerization and technologies (for instance, police databases) has a great impact in the collection and recording of police information. Hence, we explore police agents' expectations for the future management of criminal bodies in a surveillance society. The perspective of a big brother society and the evolution of science and technology appear as something that will help to face the difficulties of the future. If the traditional figure of detective is being supplanted by a hybrid figure, maybe the future will demonstrate the transience of these hybrid characteristics and the boundaries drawn between people and non-human actors.

Mega-events

Rio de Janeiro Operations Center (COR-RJ) and the comunication with society: an Actor-Network Theory study

Session: **PARALLEL SESSION 9** – Mega-events

Date and time: **26th April 2014. (09:15-10:45)**

Authors: **Alexandre Hojda and Tamiris Cunha Vaz**

The Rio de Janeiro Operations Center (COR-RJ) is a command and control center (CCC), an agency created in the logic of Smart cities to assist the management of the city, includ more than thirty different actors (human actant) and technology (non-human actants), in order to facilitate decision-making in three different dynamics: routine of the city, for emergencies and for big events (World Cup 2014 and the Olympics Games in 2016).

The focus of the study will be the analyze the use of technology in government communications (COR-RJ) with the society (and vice versa), using Actor Network Theory (ANT), and for this study, will be select some tools of Information, Communication Technologies (ICTs) as: website, electronics panels, cell phone's message, Facebook, Twitter, Waze, Youtube, Phone 1746, newsletters etc.

To the analysis will be used the framework of translation from ANT:

• The problematic: first the reasons, the problems involved in the initial decision;

• The enrollment of actors: the process of involvement and identification of the institutions involved. Bring actors to participate in the network;

• The displacement: strategies definition of roles, relations and resistances in the changes process;

• The stabilization: will the use of the communication by COR-RJ obtained the stabilization or not, It could impact in the relation between actors can destabilize the decision or (and) the network.

Is important to emphasize, that the technology is a great way to connect the public sector and society, but the use of technology should not be the panacea of the world and only use (expensive) 'Smart Cities' projects, with command and control centers, probably it will not solve the urban problems, cultural elements, infrastructure problems and empowerment of the society.

Surveillance-driven security during the spectacle: Contested control in the Olympic city

Session: **PARALLEL SESSION 9** – Mega-events

Date and time: **26th April 2014. (09:15-10:45)**

Author: **Pete Fussey**

During the summer of 2012 London hosted one of the world's largest sporting events that both served to both catalyze numerous existing processes and practices of urban surveillance in the city, and introduce other novel approaches. Drawing on data collected from empirical research during the period of Games – focusing on the application of London's 2012 Olympic security operation and of those subjected to it (including ethnographic research of police patrols, observations of CCTV suite operations and interviews with key security agencies, activists, arrestees and those subjected Olympic bail conditions) – this paper illustrates the complex, diverse and dynamic uses of surveillance practices during the period. In doing so the longstanding recognition that space is used in simultaneously diverse ways is reflected in the surveillance and control practices applied to it. Moreover, despite the professed unity of purpose among Olympic planners, more detailed analysis reveals both the application and purpose of surveillance-driven ordering processes as contested and sometimes contradictory realms. Within the burgeoning conceptual literature in this field, mega event surveillance and security practices are often characterised as an exceptional exercise in terms of scale, scope and form and considered variously through macro-theoretical lenses citing the assertion of overarching disciplinary, neo-liberal, colonial corporatist and other interest-based aspirations. Drawing on Foucauldian (2007) notions of security and more recent applications to urban surveillance practices (Klauser 2013; Fussey 2013), surveillance-driven spatial impositions of order – regulatory, exclusionary, disciplinary, suggestive and assuasive – are argued to exist simultaneously in the same broadly defined area.

Olympic "McVeillance": The 'McDonaldised Surveillance' in the post-9/11 Summer Olympics (Athens, Beijing and London) and its 'glocal' implications

Session: **PARALLEL SESSION 9** – Mega-events

Date and time: **26th April 2014. (09:15-10:45)**

Autors: **Minas Samatas**

The post-9/11 Olympic Games under the impact of terrorist threats and the interests of the

surveillance corporate giants and more broadly of the “Surveillance Industrial Complex” have been used as a prestigious testing ground for new security and surveillance systems and a showcase for global marketing of lucrative surveillance technologies and services.
We use here the term ‘McVeillance’ to refer to the global marketing and application of standardized surveillance technologies (hardwares and softwares), activities and solutions for local security needs by large multinational corporations; also by “Olympic McVeillance” we mean the Olympic security and surveillance systems and measures, which once established with an esteemed Olympic brand name, become the standardised security pattern for future Olympics, other mega-events, and yet for everyday security-surveillance needs in a global “Mc-Security” market. Hence, the Olympic security industry and the “Surveillance Industrial Complex,” which sponsor and exploit the contemporary “McDonaldized Olympics” promote all sorts of the latest surveillance technologies, from sophisticated CCTV cameras to integrated surveillance systems, GPS and dataveillance algorithms, smart cards, drones, etc., as a panacea for local security solutions. In this paper we will present distinctive “McVeillance” systems and solutions, which have been used in the Athens, Beijing and London Olympics to argue that their standardised, global extension, underpinned by the desire for profit may have serious local personal and anti-democratic implications, not excluding corruption. Because, Olympic “McVeillance” can ultimately threaten individual and civil liberties when it is used not for exceptional occasions but for everyday security needs without restrictions and privacy safeguards. In brief, the overall glocal impact of the Olympic ‘McVeillance’, which is of course depending on the local state, regime and culture, can contribute to an emerging “global surveillance society.”

Health

Caring for your Data Double: New Risks and Responsibilities in an Era of Ubiquitous Health Information Flows

Session: **PARALLEL SESSION 10** – Health

Date and time: **26th April 2014. (11:00-12:30)**

Author: **Martin French**

In the United States (US), Health Information Exchanges (HIEs) are emergent initiatives designed to pool the personal health information of individual patients in order to facilitate care. Proponents also hope that HIEs will support diverse secondary uses of health information (e.g. biomedical research, public health surveillance, comparative effectiveness research, etc.), thereby improving quality while also lowering care costs. Yet, while HIEs stand to transform systems care in some significant ways, they also generate new risks associated with the ubiquitous flows of personal health information, and new responsibilities for patients who are rendered (potentially) transparent by these flows. Using documentary evidence (and informed by debates in content- and discourse-analysis), this paper considers how HIEs are conceptualizing, addressing, and attempting to manage emergent risks. With particular attention to the ways that patients are rendered transparent—and focusing on how they are made responsible for managing the risks associated with flows of their personal health information—this paper discusses emergent strategies for protecting patient privacy. It argues that these strategies privilege technically literate and digitally enabled citizens, while also potentially marginalizing those unable to sufficiently care for their data doubles.

Catching the Flu: Early Warning Surveillance Systems for Detecting Pandemic Outbreaks

Session: **PARALLEL SESSION 10** – Health

Date and time: **26th April 2014. (11:00-12:30)**

Autors: **Stefan Elbe and Stephen Roberts**

How can intentional or unintentional infectious disease outbreaks be detected more rapidly around the world? Policy-makers working on pandemic preparedness have a keen interest in rapid detection of new infectious disease outbreaks – both in order to gain more time to prepare their own countries against a new pandemic, and in order to contain any new outbreak at source.

However, in many parts of the world surveillance system are patchy, and there are also economic and political disincentives for rapid notification of new infectious disease outbreaks. In this context, a number of new internet-based early warning systems have been developed using a new method of surveillance – 'syndromic' surveillance – which function through (near) real-time monitoring of a range of non-health specific data sources that might indirectly indicate a new outbreak through revealing unusual clusters of more general symptoms. The purpose of this paper is to (1) identify the array of new syndromic surveillance technologies that have been pioneered over the past decade in the field of pandemic preparedness; (2) to illustrate how these new technologies operate according to different principles of diseases management when compared to earlier reporting systems; and (3) to contextualize the emergence of these new health security technologies within what this paper calls the 'medicalization of insecurity'.

Surveillance cultures, public health and public order: inter-agency liaison and information-sharing in policies towards drug users in Amsterdam (Netherlands) and Porto Alegre (Brazil)

Session: **PARALLEL SESSION 10** – Health

Date and time: **26th April 2014. (11:00-12:30)**

Autors: **Rafaela Rigoni**

If surveillance is understood as a complex multi-dimensional process, then collaboration between health, social and law enforcement sectors, can be viewed as a part of the surveillance culture of particular societies and urban settings. Policies towards illicit drugs are usually build on a two-track approach – public health and public order – which brings different objectives that have to be negotiated daily by street level workers. In this paper we use examples of collaboration among workers from social, health and law enforcement sectors in Amsterdam, the Netherlands, and Porto Alegre, Brazil in their daily approach of drug users, to analyze the types of surveillance arising from these negotiations. The study is part of a qualitative PhD research where 80 in-depth interviews with street level workers and 800 hours of participant observation were carried out from February 2010 until March 2011, equally divided between the mentioned cities. Different cultures of surveillance produce diverse consequences for drug users in terms of welfare access and empowerment. In Amsterdam, the close collaboration and information exchange among workers produce a 'chain' culture: an intensive screening allows drug users to have more access to care, yet, at the same time this promotes excessive control towards them. Extreme control, eventually, can divert users from care and produce a power shift towards repression and dependency within a

public health and empowerment drug policy. In Porto Alegre, on the other hand, insufficient collaboration produces a surveillance culture of 'holes': less systematic screen and information sharing allow users to slip out of care, but also to have more room of maneuver to decide upon their lives, independently from government's expectations. Historically coming from opposite extremes in terms of drug surveillance (respectively permissive and controlling), Amsterdam and Porto Alegre have been walking towards each other to meet somewhere in the middle.

User-led surveillance

Tracking the State: Could civic driven visibility of government reverse a historical trend?

Session: **PARALLEL SESSION 10** – User-led surveillance

Date and time: **26th April 2014. (11:00-12:30)**

Author: **Christiana Maria Mauro**

Just as digital media's long tail business model is putting an end to the conditions that have allowed mass culture to exist for the past 200 years, through the same statistical logic equal potential exists to erode entrenched institutions and shape political structures. The state has always controlled the ability to shape society into something legible. Its executive powers and resources have equipped it to do so. But today the digitalization of public records, freedom of information laws, encryption technology and cheap technological infrastructure have created viable tools for generating legibility of the activities of government. Through developments such as Wikileaks, corruption mapping and other crowd-sourced resistance activities, civil mobilization is beginning to erode some of the institutional conditions that historically have enabled the state to remain so resistant to bottom-up reform. Online interpersonal communication between entities engaged in civic activism are transforming the orientation of behavioural tracking. This talk will offer a sociological perspective on this budding phenomenon with a number of examples of movement entrepreneurship.

Examining private uses of surveillance technology

Session: **PARALLEL SESSION 10** – User-led surveillance

Date and time: **26th April 2014. (11:00-12:30)**

Author: **Liisa A. Mäkinen**

This paper examines how people use surveillance technology, especially surveillance cameras for their own purposes. In Finland a number of people have installed cameras and other surveillance systems in private premises since the technology has become available to them. For instance, homes are equipped with surveillance systems connected to a company providing security services; heat-activated online cameras are installed in summer houses in the countryside; and webcams are used when monitoring other places where private property is kept. These systems can be considered as archetypal surveillance as they are installed and operated for security reasons. However, as they are used by private individuals for private purposes they deserve a more thorough scrutiny.

The data used in this research consists of interviews on people who use this type of surveillance equipment. This paper aims to deepen the understanding of participation of individuals in surveillance. Through interviews I examine why these people chose this surveillance method, and how they use it. I consider whether this type of private use of technology changes the interviewees' experience of surveillance in whole, and if the surveillance produced here is the same in nature as traditional video surveillance is.

Space, location

Going into Witness Mode: Anticipating Electronic Evidence

Session: **PARALLEL SESSION 10** – Space, location

Date and time: **26th April 2014. (11:00-12:30)**

Authors: **Lonneke van der Velden**

This paper discusses the ways in which a mobile phone application, InformaCam, creatively turns a problem, that of mobile device tracking, into a method of public proof. The widespread use of mobile devices by human rights activists and organizations has raised a new set of concerns. First, mobile devices, and the communication they allow for, can be easily tracked. Second, the documentation that is produced by mobile devices is often instable: because digital material is vulnerable to manipulation, verifying its authenticity has become key. Against this backdrop, citizen journalists and human rights activists are faced with the question of how to prove the truth of an event using digital technologies without being traced themselves.

InformaCam, developed by The Guardian Project, deals with metadata, potentially identifying information hidden in the make-up of a file. When posting images or videos online one likely also uploads metadata, such as GPS data, along with it. InformaCam allows users to remove metadata and to diminish the chance that they can be identified or located. However, InformaCam also makes a second version of the image. In this version, contextual metadata, such as the time stamp or the Cell ID (of GSM masts), is not obscured but deliberately captured, encrypted and stored. One could even add specific metadata about the setting in which the image was taken and annotate the images with the help of embedded categories that legal experts consider relevant.

InformaCam makes surveillance tangible and mobilizes the tracking capacity of mobile devices for the sake of producing potential evidence. Inspired by the work of Bruno Latour, Gabriella Coleman and Susan Schuppli, the paper shows how establishing this move entails the inscription of legal formats, seeking a public, and experimentally contributing to a new material-legal culture of witnessing.

Cross-cultural Perspectives on Surveillance, GPS, Geolocation, Technologies, and Privacy

Session: **PARALLEL SESSION 10** – Space, location

Date and time: **26th April 2014. (11:00-12:30)**

Authors: **Barbara Burke**

Abstract for 6th International Surveillance and Society Conference Visiting Associate Professor Barbara Burke, Arizona Summit School of Law October 3, 2014.

The collision of citizens' privacy expectations and the rights and acceptable parameters of GPS, geolocation technologies, and other technological and non-technological surveillance modalities triggers a global conversation. This paper will discuss the history of the use and governance of such technologies in several cultures, as well as the various approaches to the politics and practicalities of regulating surveillance, both in government and private sectors. The paper next focuses on current standards and practices regarding data and knowledge protection, and then addresses ongoing efforts to regulate surveillance within and amongst sovereigns. A discussion of the need for treaties, memoranda of understanding, and international cooperation in developing standards in regulating surveillance concludes.

Private video monitoring of public spaces: the construction of new invisible territories

Session: **PARALLEL SESSION 10** – Space, location

Date and time: **26th April 2014. (11:00-12:30)**

Authors: **Rodrigo Jose Firmino and Fábio Duarte**

Besides the hype and enthusiasm surrounding the possibilities of an increasing capacity for "central" control of the city justified by the dream of smart urbanism, the city is also made up of a series of scattered networks of technologies and practices (associated with these technologies). These form a fluid network of devices and systems that participate in the formation of an intangible territorial layer made of ephemeral appropriations of space with various levels of interconnection, systematization and complexity. We believe there is an informal and unnegotiated form of territorialization—part of what David Lyon and Zygmunt Bauman call "liquid surveillance"—that is fundamentally supported by the possibilities for smarter control over actions in the urban space offered by ever smaller and more invisible technologies. This is more evident in the surveillance

practices of private actors directed toward the public space. Much has been said (and studied) about the use of surveillance in public spaces by the government or in private spaces by private security companies. We concentrate our hypothesis of a new territorial layer on the use of surveillance in public spaces managed and controlled by private actors, with the tacit consent of the State. The making of geographical territories in the city can be seen as a sociotechnical process that

involves an overlapping of different physical, legal, cultural and technological interconnected layers. A constellation of small, medium and large private security companies – and in many cases, individuals – are “in charge” of monitoring spaces that were supposed to be public, free from any kind of private control. In the logic of the territorial layers, this “private management of public spaces” can be seen as yet another coating in the making of urban territories. We seek to question this relation by making reference to several specific uses of ICTs for surveillance purposes and to discuss it from the point of view of definitions of space, place and territory.

Consumption

John and Jane Doe meet the Copyright Surveillance Industry

Session: **PARALLEL SESSION 10** – Consumption

Date and time: **26th April 2014. (11:00-12:30)**

Author: **Mike Zajko**

With few exceptions, the field of surveillance studies has neglected the development of monitoring systems tied to intellectual property rights. This paper assesses the growth of the global copyright surveillance industry, its drivers, and the consequences of these developments for individuals and online flows of cultural products. In particular, my focus is on the companies that track the online distribution of copyrighted works, their relationship with copyright owners, and the integration of these services with national-level enforcement and policing strategies. Many of these private surveillance programs are extensive and highly automated. They have been criticized for enabling preemptive enforcement and the reverse onus placed on alleged infringers. When copyright surveillance services have been used to provide evidence for civil court cases, they have raised fundamental questions about the nature of identification and attribution on the internet. These concerns over digital identification are significant beyond the realm of copyright enforcement. While copyright surveillance programs have a number of uses, including market research and justifying regulatory intervention, my main focus is on their use in effecting controls on content distribution and as part of revenue-generating schemes involving courts. This paper also includes a case study of an ongoing civil suit that is setting an important precedent in Canada. I argue that the financial interests motivating copyright surveillance suggest further expansion and technological refinement in this domain, but the dependence of such systems on an enabling regulatory framework makes them vulnerable to increasingly sceptical publics and legal authorities.

Cultures of consumption within GPS speedsurfing

Session: **PARALLEL SESSION 10** – Consumption

Date and time: **26th April 2014. (11:00-12:30)**

Author: **Karl Palmås**

The phenomenon dubbed “the quantified self movement” is gathering pace and increasingly making headlines in popular media. There is now a wide variety of communities that measure different aspects of their bodies and lives, sharing the results online, turning it into “big data”. Outside observers have pointed to the apparent narcissism of such practices – and indeed, one

can imagine a number of theoretical prisms through which to analyse this phenomenon.

This paper, however, focuses on how the community members themselves experience such self-measurement. Based on a participant observer, micro-ethnographic study of windsurfers that use GPS devices to monitor and share the details of their windsurfing sessions, it questions the extent to which concepts like narcissism or alienation are useful for describing the practices in question.

The paper suggests that the prime effect of the introduction of GPS tracking is the establishment of an objective measure of skills and aptitude. This, in turn, prompts a heightened desire for state-of-the-art equipment. In other words, the dispersion of self-measurement technology has democratised competitive speedsurfing, but at the same time sharpened the element of competitive consumption within the sport. Beyond the description of the community in question, the paper also reflects upon whether these findings can be applied to the self-quantification movement and its place within the contemporary economy.

Materiality matters: Limitations and possibilities in consumer surveillance configurations

Session: **PARALLEL SESSION 10** – Consumption

Date and time: **26th April 2014. (11:00-12:30)**

Author: **Jason Pridmore**

Though sometimes ignored, particularly given the focus on ‘sensational’ possibilities of surveillance through new technologies, materiality plays a crucial role in everyday practices of surveillance. From broken cameras to missed communications between key personnel to the size of storage on hard drives, surveillance(s) is (are) dependent on an interconnected network of (human and non-human) actors. This paper will examine some of how material arrangements in practices of consumer surveillance at times mitigate its potential and at times enhance or increase its use.

The paper looks at three specific areas in which ‘materiality matters’ for practices of consumer surveillance: social media infrastructures, legacy systems, and employee tacit knowledge (of systems). The development of social media has allowed for and unprecedented collection of information in the everyday lives of users/consumers. However the interconnected processes that enables the sharing of this information, for example in creating personalized services based on social media profiles, requires a significant amount of work. This work limits the ability of companies to ‘effectively’ deploy modes of consumer surveillance based on social media, and their marketing plans often lag behind new trends in social media. A number of companies are also often limited in their monitoring of and marketing to consumers because of the lack of integration with or

upgrading of their legacy systems. Despite the goals for fully integrated systems advocated in business literature, such as the use of Customer Relationship Management softwares, legacy systems and additional developments such as the advent of social media channels only make this integration increasingly difficult. On the other hand, increased storage capacities and non-systematic approaches to data protection mean that these materialities significantly increase potentials for a continuing and pervasive surveillance. Possibilities are also mitigated by technical know-how and expertise, indicating yet another way in which materiality matters for surveillance. The tacit knowledge of employees is a crucial element in surveillance practices, as they have an understanding of what can be done and what cannot be done within present system configurations.

The implications of this research suggest that a more fully developed and 'thick' description of practices of surveillance (in this case of consumer surveillance) can temper some of the most significant concerns raised by surveillance studies scholars and raise other issues potentially overlooked.

By authors

Dietmar Kammerer – 26th April 2014. (11:00-12:30)
Dimitris Gritzalis – 25th April 2014. (17:00-18:30)
Dimitris Tsapogas – 26th April 2014. (11:00-12:30)
Elin Palm – 25th April 2014. (13:30-15:00)
Elonnai Hickok – 25th April 2014. (09:15-10:45)
Elvira Santiago – 24th April 2014. (13:00-14:30) – 24th April 2014. (13:00-14:30)
Emmeline Taylor – 25th April 2014. (15:15-16:45)
Eric Stoddart – 25th April 2014. (17:00-18:30)
Eric Toepfer – 24th April 2014. (14:45-16:15)
Eveline Lubbers – 25th April 2014. (17:00-18:30)
Fábio Duarte – 26th April 2014. (11:00-12:30)
Fiona de Londras – 24th April 2014. (14:45-16:15)
Francesca Menichelli – 24th April 2014. (10:30-12:00)
Francisca Grommé – 25th April 2014. (13:30-15:00)
Francisco Klauser – 25th April 2014. (09:15-10:45)
Fredrika Björklund – 24th April 2014. (13:00-14:30) – 25th April 2014. (17:00-18:30)
Gabriel Bartl and Lars Gerhold – 24th April 2014. (10:30-12:00)
Gavin John Douglas Smith – 25th April 2014. (17:00-18:30)
Gemma Galdon Clavell – 25th April 2014. (11:00-12:30) – 25th April 2014. (13:30-15:00)
Gary Edmond – 25th April 2014. (09:15-10:45)
Gloria Gonzalez Fuster – 25th April 2014. (11:00-12:30)
Göran Bolin – 24th April 2014. (10:30-12:00)
Goupy Marie – 24th April 2014. (13:00-14:30)
Greg Elmer – 25th April 2014. (11:00-12:30)
Harrison Smith – 25th April 2014. (11:00-12:30)
Hedenus Anna – 25th April 2014. (15:15-16:45)
Helena Machado – 26th April 2014. (09:15-10:45)
Hee Jhee Jiow – 25th April 2014. (17:00-18:30)
Ivan Szekely - 25th April 2014. (09:15-10:45)
J. Peter Burgess – 24th April 2014. (10:30-12:00)
James Martin – 25th April 2014. (13:30-15:00)
Jane Bailey – 25th April 2014. (17:00-18:30)
Jason Derby – 24th April 2014. (13:00-14:30)
Jason Pridmore – 26th April 2014. (11:00-12:30)
Jeffrey Monaghan – 24th April 2014. (13:00-14:30) – 25th April 2014. (11:00-12:30)
Jens Hälterlein – 25th April 2014. (11:00-12:30)
Johann Chaulet – 25th April 2014. (17:00-18:30)
John Tucker – 24th April 2014. (14:45-16:15) – 24th April 2014. (14:45-16:15)
Jonas Andersson – 24th April 2014. (10:30-12:00) – 24th April 2014. (13:00-14:30)
Jonathan Naveh – 25th April 2014. (17:00-18:30)
Juha Vuori – 25th April 2014. (09:15-10:45)
Julian Staben – 25th April 2014. (15:15-16:45)
Jutta Weber – 25th April 2014. (15:15-16:45)
Karl Palmås – 26th April 2014. (11:00-12:30)
Katja Lindskov Jacobsen – 24th April 2014. (10:30-12:00)
Keith Spiller – 25th April 2014. (13:30-15:00)
Kerrin-Sina Arfsten – 24th April 2014. (14:45-16:15)
Kevin Donovan – 26th April 2014. (09:15-10:45)
Kevin Haggerty – 24th April 2014. (09:00-10:15h)
Kevin Walby – 24th April 2014. (13:00-14:30)
Krista Craven – 25th April 2014. (17:00-18:30)
Kristel Beyens - 25th April 2014. (11:00-12:30)
Kirstie Ball – 25th April 2014. (13:30-15:00)
L Muir – 24th April 2014. (14:45-16:15)
Lachlan Urquhart – 25th April 2014. (17:00-18:30)

Lars Ostermeier – 24th April 2014. (14:45-16:15)
Laura Gracia – 24th April 2014. (10:30-12:00)
Lauri Paltemaa – 25th April 2014. (09:15-10:45)
Liisa A. Mäkinen – 26th April 2014. (11:00-12:30)
Lilian Edwards – 25th April 2014. (17:00-18:30)
Lilian Mitrou – 25th April 2014. (17:00-18:30)
Liliana Arroyo Moliner – 25th April 2014. (13:30-15:00)
Liz Daniel – 25th April 2014. (13:30-15:00)
Lonneke van der Velden – 26th April 2014. (11:00-12:30)
Lucas Melgaço – 24th April 2014. (10:30-12:00)
Malavika Jayaram – 26th April 2014. (09:15-10:45)
Marc Kosciejew – 24th April 2014. (10:30-12:00)
Marc Ménard – 24th April 2014. (13:00-14:30)
Mari-Liis Madisson – 24th April 2014. (13:00-14:30)
Maria Angeles Martinez Serrano – 25th April 2014. (09:15-10:45)
Marie-France Lebouc – 25th April 2014. (15:15-16:45)
Marijke Roosen - 25th April 2014. (11:00-12:30)
Martin French – 26th April 2014. (11:00-12:30)
Matthew Hoye – 25th April 2014. (11:00-12:30)
Matthias Schulze – 24th April 2014. (10:30-12:00)
Maude Bonenfant – 24th April 2014. (13:00-14:30)
Maureen Meadows – 25th April 2014. (13:30-15:00)
Maxime Ouellet – 24th April 2014. (13:00-14:30)
Mehera San Roque – 25th April 2014. (09:15-10:45)
Michael Dahan – 26th April 2014. (09:15-10:45)
Miguelángel Verde Garrido – 24th April 2014. (10:30-12:00)
Mike Nellis – 25th April 2014. (11:00-12:30)
Mike Zajko – 26th April 2014. (11:00-12:30)
Miltiadis Kandias – 25th April 2014. (17:00-18:30)
Minas Samatas – 26th April 2014. (09:15-10:45)
Mirjam Puumeister – 25th April 2014. (17:00-18:30)
Mohammed Masoodi – 24th April 2014. (14:45-16:15)
Morten Hjelholt – 26th April 2014. (09:15-10:45)
Mouli Bentman – 26th April 2014. (09:15-10:45)
Nelson Arteaga-Botello – 24th April 2014. (14:45-16:15)
Niklas Creemers – 25th April 2014. (11:00-12:30)
Nils Zurawski – 25th April 2014. (11:00-12:30)
Noellie Brockdorff – 25th April 2014. (11:00-12:30)
Ola Svenonius – 24th April 2014. (13:00-14:30) - 25th April 2014. (17:00-18:30)
Olga Galanova – 24th April 2014. (10:30-12:00)
Ott Puumeister – 25th April 2014. (17:00-18:30)
Patrick Murphy – 24th April 2014. (10:30-12:00)
Paul De Hert – 26th April 2014. (11:00-12:30)
Pawel Waszkiewicz – 24th April 2014. (13:00-14:30) – 25th April 2014. (17:00-18:30)
Pedro Sanches – 25th April 2014. (11:00-12:30)
Pete Fussey – 26th April 2014. (09:15-10:45)
Peter Marks – 24th April 2014. (13:00-14:30)
Philip Boucher – 26th April 2014. (09:15-10:45)
Pinelopi Troullinou – 25th April 2014. (11:00-12:30)
Priscilla Regan – 25th April 2014. (17:00-18:30)
Priya Dixit – 25th April 2014. (09:15-10:45)
Rachel Dubrofsky – 25th April 2014. (09:15-10:45)
Rafaela Rigoni – 26th April 2014. (11:00-12:30)
Raphaël Gellert – 25th April 2014. (11:00-12:30)
Raul Gschrey – 24th April 2014. (10:30-12:00)

Raymond Liedka – 24th April 2014. (13:00-14:30)
Regina Berglez – 26th April 2014. (09:15-10:45)
Reinhard Kreissl – 25th April 2014. (09:15-10:45)
Renee Powers and Alessandro Panebianco – 25th April 2014. (15:15-16:45)
Ricardo Medeiros Pimenta – 24th April 2014. (10:30-12:00)
Richard Jones - 25th April 2014. (09:15-10:45) – 25th April 2014. (13:30-15:00)
Rick Linden - 25th April 2014. (15:15-16:45)
Roberta Michel – 24th April 2014. (13:00-14:30)
Rocco Bellanova – 25th April 2014. (11:00-12:30)
Rodrigo Jose Firmino – 26th April 2014. (11:00-12:30)
Rosa María García Sanz – 25th April 2014. (13:30-15:00)
Rosamunde Van Brakel - 25th April 2014. (17:00-18:30) – 26th April 2014. (11:00-12:30)
Roy Coleman – 25th April 2014. (09:15-10:45)
Rozemarijn van der Hilst – 24th April 2014. (14:45-16:15)
Rune Saugmann Andersen – 24th April 2014. (10:30-12:00)
Saif Haq – 26th April 2014. (09:15-10:45)
Sally Dibb – 25th April 2014. (13:30-15:00)
Salvatore Iaconesi and Oriana Persico – 25th April 2014. (13:30-15:00)
Sami Coll – 24th April 2014. (14:45-16:15)
Sandra Appleby-Arnold – 25th April 2014. (11:00-12:30)
Sara Degli Esposti – 24th April 2014. (14:45-16:15) – 24th April 2014. (13:00-14:30)
Scott Thompson – 24th April 2014. (10:30-12:00)
Shoshana Magnet – 25th April 2014. (09:15-10:45)
Solon Barocas – 24th April 2014. (14:45-16:15)
Sofia Morales – 25th April 2014. (17:00-18:30)
Sonja Snacken - 25th April 2014. (11:00-12:30)
Sophie Stalla-Bourdillon – 24th April 2014. (13:00-14:30)
Stefan Elbe – 26th April 2014. (11:00-12:30)
Stephen Roberts – 26th April 2014. (11:00-12:30)
Susanne Wigorts Yngvesson – 25th April 2014. (15:15-16:45)
Tamiris Cunha Vaz – 26th April 2014. (09:15-10:45)
Thomas W. Lauer – 24th April 2014. (13:00-14:30)
Tj McIntyre – 25th April 2014. (15:15-16:45)
Tjerk Timan – 25th April 2014. (09:15-10:45)
Torin Monahan – 25th April 2014. (17:00-18:30)
Val Steeves – 24th April 2014. (09:00-10:15h)
Valeria Ferraris – 25th April 2014. (11:00-12:30)
Valerie Steeves – 25th April 2014. (17:00-18:30)
Victoria Wang – 24th April 2014. (14:45-16:15) – 24th April 2014. (14:45-16:15)
Vincenzo Pavone – 24th April 2014. (13:00-14:30)
Vlad Niculescu-Dinca – 25th April 2014. (09:15-10:45)
Wil Chivers – 24th April 2014. (10:30-12:00)
William Lockrey – 25th April 2014. (11:00-12:30)
William Webster - 24th April 2014. (13:00-14:30) – 25th April 2014. (13:30-15:00) - 25th April 2014. (15:15-16:45)
Wook Inn Paik – 24th April 2014. (10:30-12:00)
Xavier L'Hoiry – 25th April 2014. (13:30-15:00)
Yutaka Kusajima – 24th April 2014. (14:45-16:15)