eticas
Research & Consulting

SSN
SURVEILLANCE
STUDIES
NETWORK

BOOKLET OF ABSTRACTS

ABSTRACTS

Trust and Surveillance

Explaining your Data Double: Confessions, honesty and trust in job recruitments

Anna Hedenus, anna.hedenus@gu.se, University of Gothenburg
Christel Backman, christel.backman@gu.se, University of Gothenburg

Using cybervetting as part of their recruitment process, recruiters sometimes come across information that undermines the trustworthiness of job applicants. In these cases, recruiters will either discard or follow up on the found information with the candidate (Backman and Hedenus 2014). While online searches, in a Foucauldian sense, can be categorized as a form of examination, the follow up is instead construed as a confession (Foucault 1990; Townley 1994). The aim of this paper is to study how these confessions are used and evaluated in recruitment processes and in relation to additional information accessed about the candidate. Analyses of qualitative interviews with 38 Swedish HR professionals, hiring managers and employers, show that the outcome of these confessions, functioning also as a test of the jobseeker's honesty, moral judgement and self-reflection, is crucial for the recruiters' hiring decisions. Furthermore, the need for more explicit confrontations is accounted for by a skeptical attitude to the reliability of various online sources, calling for ways to verify or disprove the information. The confession also becomes an opportunity for the applicants to "come clean" about their past and freely share unfavorable information about themselves to the recruiters. Hence, cybervetting as a surveillance practice, with the recruiter examining jobseekers also in more private spheres, has direct consequences on recruitment as well as clear effects on jobseeker's self-examination, real life interactions and HR management.

Coming to terms with seductive surveillance; rationalisation and resistance: a qualitative study on the subjective experience of surveillance through smartphone devices.

Pinelopi Troullinou, p.troullinou@gmail.com, Open University, Business School

In the context of neoliberal capitalism the traditionally distinct spheres of security and marketing have merged and so have the respective means. Surveillance in the digital era has become ubiquitous and an integral part of modern societies with "our whole way of life in the contemporary world [being]

suffused with surveillance" (Lyon, 2007: 25). Edward Snowden in his interviews has claimed that 1984 techniques of surveillance seem unimaginative as nowadays people buy their cell phones, which he equals to a networked microphone that we carry around voluntarily (The Guardian, 2014). He recently (October 2015) revealed that the UK intelligence agency GCHQ "had the power to hack into phones without their owners' knowledge" (BBC, 2015). At the same time the Ofcom Communications Market Report in August 2015, announces the UK as a "smartphone society". According to the report, "smartphones have become the hub of our daily lives and are now in the pockets of two thirds of UK adults" while the absolute majority (90%) of 16-24 years olds own one. Individuals feed the surveillance mechanism themselves with ever more personal data through their activities on digital devices. However, does this imply that young users do not care about surveillance, or their privacy? This paper aims to address the subjective experience of surveillance using smartphone devices as a case study. Smartphones are not explicitly a means of surveillance and are not perceived as such by users. However, as argued above, the data collected by these devices can be used both by the market and the state for marketing and security purposes. Drawing upon the findings of 13 focus groups conducted amongst students in British Universities, I will argue that participants relate the privacy concerns with trust in relevant organizations. Furthermore, they feel responsible for their data management adopting a discourse of responsibilization emerging from the neoliberal ideology. In this context, resistance is related to responsibility when exposing oneself and thus self-censorship is interestingly employed as the main strategy of resistance.

Democracy without surveillance: Trust in P2P infrastructure.

Simone Belli, sbelli@yachaytech.edu.ec, Yachay Tech

We present a case-study which is part of a research project based in Spain, and carried out between 2011 and 2014. The project's focus was on social institutions and affective processes involved in what is normally referred to social movements. Using extracts from narrative interviews, we explore how participants in social protest cross attachment and technology in order to develop trusting relationships. We consider technology as markers of the emergence of new forms of cooperation and innovation constructed by shared trust among the actors involved in social institutions. We argue that trust is built between actors and devices involved in democracy without surveillance, including emergent modalities of democratic action. So the research problem for us is to understand how trust can be recovered in social institutions and for this we show different types of innovative and creative process born from indignados movement. Within the frame of this article we focus our attention on a specific corpus, that of interviews with experts (activists, hackers, communicators, journalists, etc.)

belonging to an innovative and creative social institution represented by the movement. Where subjects design in their narratives a form of sharing knowledge through a dialogical process. We present social institutions and P2P infrastructure situated within a body of work in the sociology of innovation and science and technologies studies, conduced recently on the topic of horizontal technology. We analyze the "stabilization" of the innovation used with the establishment of a configuration in which the tool and infrastructures become transparent and invisible. Finally, we show the results of our research introducing a specific device, dynamic or practice as being in some way related to trust, the expert knowledge contributes to the very definition and shaping of this trust within a democracy without surveillance.

The surveilled subject and relational models of procedural justice

Alana Saulnier, 12as32@queensu.ca, Queen's University

Understandings of surveilled subjects' experiences with surveillance remain nebulous and discrete in the surveillance studies literature. This research points to relational models of procedural justice as a consistent theoretical explanation of surveilled subjects' experiences in similar but distinct surveillance contexts. Some efforts have been made to understand experiences with surveillance through an organizational procedural justice framework (Alge, 2001; Ball, 2001; 2002; 2012). Ball's contributions are particularly important; highlighting the relationship between perceptions of surveillance procedures and perceptions of surveillance outcomes for surveilled subjects (especially voice and implications of process/outcome control – non-relational concerns). However, relational models of procedural justice stress that the relationship between processes and outcomes are based on relational concerns, specifically: (1) neutral and consistent treatment; (2) trust in administrator benevolence; and (3) interactions demonstrative of respect and dignity (Lind & Tyler, 1988). The relevance of these concerns to surveilled subjects' encounters with surveillance is explored qualitatively in this research. Participants (n = 47) described their encounters with surveillance in a specific (Pearson International Airport, Toronto, Canada) and general (daily life) context. The results reveal that relational models of procedural justice offer a mechanism for consistently understanding and potentially predicting surveilled subjects' perceptions of and reactions to surveillance across varied contexts, but particularly those that involve a direct interaction with an authority figure acting as an agent of surveillance. Specifically, relational concerns may affect surveilled subjects' satisfaction with, acceptance of, and support for the application of surveillance as well as administering authorities based on existing procedural justice research. I argue that encounters with surveillance should be designed with their consequences in mind, which necessitates understanding

the qualities of surveillance procedures that affect surveilled subjects' perceptions of and reactions to those encounters. Specific implications and future directions of the research are discussed.

Spying Between Citizens and Allies in the Age of Insecurity: 'Glocal Coveillance' Beyond Any Trust

Minas Samatas, samatasm@uoc.gr, University of Crete

Although citizens watching citizens (CWC) and spying between allies are not unusual and both are going on for centuries, they have been lately developed and normalized due to the growing insecurity in local and global scale. Locally, in many democratic societies following neoliberal policies CWC is encouraged by the authorities and adapted by citizens and communities. In the global level, as the Snowden revelations have confirmed, the US has practiced bugging of its European allies, which are also mutually spying. This study will try to analyse the logic, causes and effects of this kind of "glocal coveillance," reflecting an emerging 'glocal' surveillance society without any trust and democratic accountability. Our analysis will be based on a cross-country comparison between the UK and Greece. In UK, CWC has become normalized since the 1980s and also UK actively participates in the US-led spying on enemies and allies alike. In Greece, a post-authoritarian society, CWC has failed during this current austerity period, and this country has been repeatedly victim of allies spying. Hence, our comparison will elucidate the societal, cultural, historical and geopolitical reasons of the growth, success and failure, as well as the implications of this 'glocal coveillance.'

Trust and surveillance: Maintaining the civil society

Kristene Unsworth, unsworth@drexel.edu, Drexel University

This paper will examine individual action and responsibility via civil society to address the practice and degree of surveillance in our societies. To do so, I will take an empirical and normative perspective (Matzner, forthcoming) that will draw on Giddens themes of security versus danger and trust versus risk (Giddens, 1990) to ask to what extent can or should we take as members of civil society to influence policy decisions in an era of ubiquitous surveillance and decreasing trust? Are we surprised that our governments, consumer marketing agencies and others are using the data we create via our interactions with technology? Data is ubiquitous. Very few of us are in a position today where we can move through our lives without leaving some kind of data trail. Our movements and interactions produce data points that can be scraped, cleaned, and mined by curious researchers, consumer marketing groups, and the state. How marketing organizations use our

personal data as well as how researchers use this type of data has been discussed in depth by many scholars. We also know that the state uses our personal information for identifying everything from neighborhoods with high crime rates or pollution densities to predicting criminal activity. When we question the reach of government use of personal data the “just trust us” argument has often been given. Although the increased ability for the government to conduct wide-spread surveillance is troubling; the fact that the systems are being developed and implemented should not be surprising. The potential danger that government agents may overstep their authority is clearly recognized and addressed in democratic constitutions. These documents are based on a strong skepticism of power and demand public participation.

The “Trust Effect” in Comparative Surveillance Studies: The Like Fish in Water Survey

Ola Svenonius, ola.svenonius@sh.se, Södertörn University
Fredrika Björklund, fredrika.bjorklund@sh.se, Södertörns högskola
Pawel Waszkiewicz, p.waszkiewicz@wpia.uw.edu.pl, University of Warzaw

Recent years have witnessed not only revelations about major covert surveillance operations on an international scale, but also an expanded academic interest in comparative, quantitative, surveillance studies. Several large FP7 projects that focused on surveillance recently came to an end, and initial results point to the salience of trust variables for opinions on surveillance (Van Lieshout och Friedewald 2014). However, measures of trust appear to be somewhat underdeveloped, and there is typically no possibility to produce more fine-grained analyses of the “trust effect”. Parallel to the large EU-FP7 surveys, the project Like Fish in Water: Surveillance in Post-Communist Societies commissioned field work in Estonia, Poland, and Serbia during Winter 2014-15. A representative and probabilistic sample of 1000 respondents from each country were interviewed face-to-face on matters of trust, surveillance, and topics more specific to the post-communist context. The Like Fish in Water survey enables us to differentiate between different kinds of trust (interpersonal, selective, and institutional), as well as distinguishing between a number of different public institutions. The aim of this paper is to contribute to a more qualified discussion on the “trust effect” and continue the work to expand the state of academic knowledge. The Like Fish in Water survey also includes a range of issues specific to the post-communist context, which we explore in relation to the issue of trust. How does experience from being monitored by intelligence agencies during communism play out in forming an opinion on contemporary surveillance? How do corruption impact on trust and acceptance of various kinds of surveillance practices? How do ethnic minorities in post-communist societies

differentiate from the majority populations in terms of trust and surveillance? These are context-specific questions that are addressed in the paper, which are also of general interest in the surveillance studies.

Can trust in surveillance technologies be enhanced through certification? Lessons from the CRISP project

Thordis Sveinsdottir, thordis.sveinsdottir@trilateralresearch.com, Trilateral Research & Consulting

This paper will reflect on whether certification of technologies used for surveillance, which takes into account evaluation of social dimensions such as trust and freedom infringement, can serve to improve surveillance practices and products and thus increase the trust of citizens. It will present findings from the research phase of the FP7 funded project CRISP, which aims to produce a new pan-European certification scheme for security products, systems and services based on an evaluation of the aforementioned social dimensions. The focus of this paper will be on discussing the results of case study research of video surveillance cameras (CCTV) and Remotely Piloted Aircraft Systems (RPAS) used for surveillance. Research findings indicate that stakeholders have trust in current certification systems and seals, and see it drive good practice and improved services and product standards. Certification is also seen to enhance responsible practices and strengthen accountability in instances of wrongdoing. This paper will critically assess whether certification of surveillance products, services and systems, which is built on evaluation of social dimensions, has the potential to drive comprehensive control and guidance of practices through extensive evaluation of all aspects of surveillance, e.g., technological capacity, training, practices, data collection, storage and analysis. Furthermore, we evaluate whether certification can mitigate power imbalances, potential misuse of power and biased surveillance practices on the basis of age, class, gender and 'race', which have all been found to be inherent to contemporary surveillance practices.

Digital surveillance between power and accountability

Donatella Selva, donatellaselva@gmail.com, Centre for Media and Democratic Innovation - Luiss University
Emiliana De Blasio, edeblasio@luiss.it, Centre for Media and Democratic Innovation - Luiss University

The pervasiveness of digital technologies in every aspect of human life fostered two trends of late modern societies: first, digital technologies enhance the perception of transparency and immediacy in the relationships between citizens and institutions. In effect, both top-down surveillance and bottom-up sousveillance found in digital media a good ally. Second, digital technologies are obscure socio-technical systems that require a diffused trust by their users: they are obscure because only a techno-capitalist elite has technical knowledge and financial resources to understand and modify their logics, and their power is based on users' trust because they operate in a limited accountability regime. The aim of our research is to identify actors, relationships and strategies involved in the consolidation of digital surveillance in Europe. We observed that surveillance has been mainly criticised in a privacy-security balance paradigm that assigns a leading role to States and citizens but underestimate the power of digital surveillance companies. As part of a wider research, we tracked down the network of European actors and companies working in the big data surveillance market and their connections with national and supranational regulators. At the same time, we compared how different countries, notably Italy, France and United Kingdom, articulate their own discourses about surveillance and how technologies and big data are framed in the public debate. By using a combination of quantitative and qualitative methods, we analysed more than 1500 articles retrieved from mainstream quality press, specialist business press, and influential professional blogs between 2013 and 2015. The debate especially focuses on two aspects: from the one side, on the power relations between national governments, European Union institutions and global Internet companies; and from the other side, on trust and accountability between citizens and governments.

Global Surveillance

A Faustian Bargain: The Search for Security via Surveillance in the Apple-FBI Case

Saher Naumaan, saher.naumaan@gmail.com, King's College London

The Snowden files on the NSA's front-end access to private companies and their networks disclosed that bulk interception of communications has been a principal method for intelligence agencies to access data in transit. As end-to-end encryption becomes more prevalent, network traffic becomes harder to intercept, and the value of bulk collection as a source of intelligence decreases. Targeted surveillance of data at rest through lawful interception and computer network exploitation is the government's response to the obstacles in intelligence collection. However, building surveillance capabilities into communications infrastructure through legal mechanisms raises technical, legal, and political issues. Should the government be free to demand access to private companies and individuals' data if it facilitates law enforcement efforts to prosecute crime? Through an examination of the Apple-FBI case, this paper will argue that targeted surveillance, even if permitted by law, is damaging to national security and the security of the user. While acknowledging the technical and legal aspects, this paper will focus on the broader political debate between law enforcement and intelligence agencies, technologists and private companies, and the public. What does the rhetoric of each actor—Apple, the FBI, the Department of Justice, the White House, and the technology community—say about its intentions and motivations? What impact do those have on the norms and discourse being used to shape the debate around security and surveillance? If the government deems the use of encryption as outside the national interest, can it prevent the public from using it? This paper will analyse the impact of exceptional access on US national security through the FBI's position that it is 'going dark'—or losing access to suspects' communications—and Apple's perspective that compromised encryption mechanisms will lead to weaker security, privacy, and data protection.

Escape and Control: shifting strategies of dissent and surveillance in Egypt

Stefanie Felsberger, stefanie@aucegypt.edu, Access to Knowledge for Development Center (A2K4D)

Lina Attalah, lina.attalah@gmail.com, Mada Masr

With an investigative approach at hand, we want to trace how successive Egyptians governments sought to apply surveillance mechanisms on citizens, moving between different surveillance regimes and from targeted to mass surveillance. In parallel, we look at people's strategies of escape from these shifting regimes of surveillance and control. We seek to show how both escape and control inform each other. Contrary to the perspective that resistance is a reaction to control or surveillance, we conceptualize surveillance and control as a reaction to dissent. We draw these developments by studying a number of incidents that offer a window into the evolution of the Egyptian regime's surveillance project. Through these incidents, we show the regimes' shifting strategies of surveillance, such as the different institutions of the state's positions vis-à-vis acquiring surveillance regimes, the level of coordination between them and the associated economies. We also demonstrate how these different surveillance regimes have manifested themselves in legal instruments as well as the national communication infrastructural developments. We connect these different strategies of surveillance and control with different modes of resistance to surveillance in Egypt, starting from humorous expression to ridicule censorship and the power behind it, to creative and technologically advanced ways to escape surveillance. By highlighting seminal debates such as the cyber-security enthusiasts versus the adversaries of anonymity, we tap into a whole movement of contentious politics in Egypt that is not separate from the broader surrounding dissidence. We wish to highlight how these different modes of resistance work on reconfiguring people's perception of the state. This paper will be intellectually positioned within the discursive debates of the Panopticon and its varying shifts that tap into the evolution of surveillance from being an upper invisible apparatus to a more omnipresent and palpable manifestation of disciplinary power.

Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU

Zoe Kardasiadou (FRA), zoe.kardasiadou@fra.europa.eu, European Union Agency for the Fundamental Rights

This report, drafted in response to the European Parliament's call for thorough research on fundamental rights protection in the context of surveillance, maps and analyses the legal frameworks on surveillance in place in EU Member States. Focusing on so-called 'mass surveillance', it also details oversight mechanisms introduced across the EU, outlines the work of entities tasked with overseeing surveillance efforts, and presents the remedies available to individuals seeking to challenge such intelligence activity. Protecting the public from security threats and safeguarding fundamental rights involves a delicate balance. Brutal terror attacks and technological innovations making possible large-scale communications data monitoring have further complicated the matter, triggering concerns about violations of the rights to privacy and data protection in the name of national security protection. The Snowden revelations, which uncovered extensive and indiscriminate surveillance efforts worldwide, made clear that enhanced safeguards of these rights are needed.
By demonstrating the complex considerations involved, this report underscores how difficult it can be to address what are often seen as competing priorities, and contributes to the continuing debate on how to best reconcile them.

Security

Smart, Secure, Resilient: Security and Surveillance at the 2014 World Cup in Rio de Janeiro and beyond

Dennis Pauschinger, dennis.pauschinger@gmail.com, University of Kent/University of Hamburg

In times of late modern uncertainty and risk, governments promote claims of total security and control (Boyle and Haggerty 2012). Furthermore, and especially in more recent years, increased attention has been paid to Smart City and resilience strategies that anchor these claims in positive urban development discourses. The consequences are often the slow and hidden process of introducing surveillance procedures, deployment of exceptional security measures and the widespread implementation of situational crime prevention in specific spatial settings (Coaffee and Fussey 2015).

The city of Rio de Janeiro is an excellent field of study when it comes to analysing current security and surveillance patterns in the Global South. Rio de Janeiro has not only been host to the FIFA World Cup, will organise the IOC Olympic Summer Games, but has also introduced a Smart City centre, developed a resilience strategy, and has installed one of the world's most modern public security and surveillance structures, the Integrated Command and Control Centre (CICC). In this paper I seek to analyse the ways in which the global security models associated with Sport Mega Events (SMEs), have unfold in Rio de Janeiro and how they relate to the already existing Smart City and resilience strategy in the city. The Brazilian security plan for the World Cup involved a special set of characteristics and has been based on three pillars: cooperation, policing and surveillance. Both technological surveillance and traditional forms of policing have played outstanding roles. Drawing upon seven months of fieldwork in the security forces and the surveillance buildings of Rio de Janeiro before, during and after the World Cup the paper will provide inside views of surveillance, security, and policing in a particular setting of the Global South. While the local authorities claim to have produced a secure, smart and resilient city, my fieldwork findings identified a gap between the official discourses and the ground realities on street level.

Sensing Evil: Counterterrorism, Techno-science and the Cultural Reproduction of Security

Pete Fussey, pfussey@essex.ac.uk, University of Essex

Mark Maguire, Mark.H.Maguire@nuim.ie, The National University of Ireland Maynooth

New counterterrorism systems aimed at identifying suspicious behaviour are spreading throughout the world. Many are based on behaviour detection by skilled officers; others deploy techno-scientific theories and software-mediated environments. All of these systems have raised critical questions about scientific and legal evidence; profiling, costs and effectiveness. However, much of the recent scholarship on this topic is based on second-hand information and fails to attend to key transformations in security discourses and in practice. Rather than offering just an overview and theoretical critique, this paper draws from extensive ethnographic research on counterterrorism in the UK (with reference to the broader global securityscape) and examines the phantasmagoria of fears and threats, the experimentations, myriad 'expert' theories, and productivity in this realm. In doing so, the paper examines how, beyond utilitarian notions of efficiency and security, counterterrorism practices perform multiple cultural roles for those charged with its delivery. We discuss particular examples of counterterrorism deployments and explore the production of theories

about the human in security discourses and practices. We further argue that appeals technoscience and expert/experiential-knowledge animate a range of performative roles and creative processes that generate new forms of knowledge. These in turn translate notions of anomaly into abnormality, legitimate specific forms of security action and further reinforce constructed boundaries of good and evil.

Citizens' perceptions on surveillance, privacy and security - what differences debates make

Johann Cas, jcas@oeaw.ac.at, Institute of Technology Assessment, Austrian Academy of Sciences

The proposed contribution will mainly focus on the policy relevant results of the SurPRISE project. This FP7 Security research project was concluded in 2015. SurPRISE challenged the alleged trade-off between privacy and security, largely dominating security policy-making and the development and implementation of surveillance orientated security technologies, attributing a core role to the attitudes and perceptions of citizens. Main objectives of SurPRISE were to gain deeper insights into the complex interplay of factors and criteria influencing the acceptability of security technologies and to develop recommendations for security measures and technologies that respect fundamental rights and European values. SurPRISE conducted in nine European countries Citizen Summits and Citizen Meetings, involving about 2000 participants in total. These large-scale participatory activities were full day events with alternating phases of providing information, debating issues of privacy and security in general and of specific security technologies, voting on predefined questions, and voicing own opinions and recommendations. The presentation of the final results will comprise the empirical testing of criteria and factors influencing the acceptability of surveillance based security technologies as well as the policy recommendations derived from the involvement of citizens, experts and stakeholders. In addition, the findings from the SurPRISE project will be compared with related research activities and similarities and differences will be addressed.

"It's part of the game" – Institutional Rhetorics in Legitimizing Surveillance

Roman Pauli, pauli@uni-wuppertal.de, University of Wuppertal

Tim Lukas, lukas@uni-wuppertal.de, University of Wuppertal

Peter Imbusch, pimbusch@uni-wuppertal.de, University of Wuppertal

As a reaction to the appraisal of new risks arising from crime, terrorism, natural hazards or technical disasters, the development and implementation of new and advanced security technologies for protecting critical infrastructures is often being legitimized referring to a demand for increased security. This speech act of intersubjectively constructing an existential threat to a valued referent object and, based on this, calling for urgent and exceptional measures to deal with the threat has been analyzed as a process of securitization (Buzan and Wæver 2003). In this contribution, we argue that securitization is only one part of a comprehensive set of rhetorical strategies to legitimize the implementation of advanced surveillance systems. We analyze a set of seven semi-structured in-depth interviews with experts from safety and security departments of a critical infrastructure in Italy* using qualitative content analysis (Mayring 2000). In line with Schulze's (2015) recent elaboration on the German discourse on the NSA scandal, we identify common patterns of surveillance legitimizing strategies. In addition, our results show that the demands and legitimization strategies for surveillance – as expressed by our interviewees – are embedded in specific organizational or institutional frameworks, forming what Daase (2010) calls security culture. This is of relevance especially for democratic societies, in which the legitimacy of potentially personal rights and privacy intruding security measures becomes questionable, but then, may be reinforced in referring to the very needs of a bureaucratic organization.

IR turning to the dark side. A Bourdieu-inspired analysis of the dark norm of espionage.

Matthias Schulze, Matthias.schulze@uni-jena.de, Friedrich-Schiller Universität Jena

This paper draws on the recent turn to critical norm research in International Relations and theorizes the practice of espionage and surveillance as a dark norm. Dark or bad norms often are defined ex-negativo, for example „we use the term "good" norms when speaking about human rights, and "bad" norms when referring to those ideas that contest them (Heller and Kahl 2013, 415). Bad norms are not ontologically different from „nice" norms, but stand in opposition to, and actively contest the very moral oughtness of nice norms. The re-emergence of torture within the Global War on Terror is one prominent example in the literature. However, the paper argues this definition ex negativo is not

sufficient and that a further theorization of a norm's darkness is required. For that, the paper assumes a Bourdieu-inspired perspective arguing, that a norm's darkness refers to the realm of doxa. „The doxic world is one 'of tradition experienced as a natural world and taken-for-granted', 'what goes without saying and what cannot be said for lack of an available discourse', as opposed to 'the universe of things that can be stated, and hence thought'" (Bourdieu 1977, 164-170). In other words, doxa is the uncontested, norms that are so taken for granted or internalized in a given society, that they are not questioned. This makes them hard to study. Combining Bourdieu's thinking with what Ernesto Laclau and Chantal Mouffe call hegemonic articulations, the paper presents several ways to study dark norms from a post-structuralist perspective. It shows the validity of the concept by studying one dark norm, i.e. the practice of international espionage and surveillance in statecraft. Heller, R., & Kahl, M. (2013). Tracing and understanding "bad" norm dynamics in counterterrorism: the current debates in IR research. Critical Studies on Terrorism, 6(3), 414-428. Bourdieu, P. (1977). Outline of a Theory of Practice (16). Cambridge university press.

Data-Driven Security: Politics and Objectivity

Thomas Behrndt, t.a.behrndt@student.rug.nl, University of Groningen, Research Master Student Modern History and International Relations

Despite the lack of a uniform definition of Big Data in both popular and scientific discourses, the term has captured the imagination of many on the premise of producing new kinds of objective knowledge by utilizing large data-sets. Its representation as an objective category highlights the positivist ontology underpinning most approaches to Big Data. Similarly to previous scientific revolutions, Big Data represents a new epistemological frame that is shaping the way we see and make sense of the world, as well as giving rise to new political realities. The developments around the phenomenon of Big Data raise a number of important political questions. One central problematic is the depolitization of security and security practices in the gaze of numerical abstraction. This paper inquires into the politics of data in the context of contemporary security decision-making and surveillance as a set of practices informing it. As governments have historically worked to make their societies legible in order to understand and to govern them, Big Data can be considered a consecutive step in this tradition. Big Data is proposed as a solution to a multitude of analytical, organizational, and decision-making problems. What sets Big Data apart as a governmental tool is the unprecedented ability of non-discriminatory data collection and storage in ever-increasing amounts being presented as an asset for potential future uses. As for governments, in particular with regard to security, the linkage between

Big Data and algorithmic computation provides a novel asset. Through governmental techniques such as data-mining and profiling, Big Data allows for real-time application and hence further enables pre-emptive action. Considering these developments, the paper examines the different modes of security that the new data-driven practices constitute and the kinds of epistemological shifts that are occurring as a result.

Management of Security through Surveillance in Portugal: the Data Protection Authority's perspective

Mónica Correia, monicabessacorreia@gmail.com, University of Porto

Progressively in recent years in Portugal, public authorities lean towards the broadening of their forms of intervention in public space. Based on the argument that citizens do not perceive it as a common good as they used to, it has become a vector of a sense of insecurity, representing a major challenge for urban management and proximity security. There are two different approaches to security management by public authorities: the management by punishment, which is a reactive approach; and the management by integration and proactivity, which entails a prevention approach. In this context, video surveillance arises as a strategic prevention policy. Public authorities argue that this method should be used for efficiency reasons in the management and intervention of police forces, in order to anticipate inappropriate behaviour, particularly of a collective nature, with potential dangerous consequences. In this perspective, surveillance ensures an optimal action of control and supervision that emphasizes prevention. Notwithstanding, according to the Data Protection National Authority the end treatment of video cameras has to be coordinated with the principles of necessity, pertinence and proportionality. This means that such use may only be authorized when necessary and specifically the most appropriate for maintaining security and the prevention of crime, taking into account the specific local circumstances that require monitoring. This Authority argues that since video surveillance systems involve restrictions to rights, freedoms and guarantees, the fundamental principle to hold, regarding what has been considered by the Constitutional Court, is that it will be up to the law to decide to what extent these systems may be used and to ensure that the restrictions are limited to the extent necessary to protect other rights or fundamental interests. Bearing in mind the connection between Law and Surveillance - whether their presence together is expected or in deep tension - based on legislation and internal documents from the Data Protection Authority, this paper discusses how its perspective and security's management using surveillance

are related in Portugal. Likewise, it debates the main challenges that the legal framework about surveillance establishes for management when security is concerned.

Vigilantism and Vigilance

Digital Vigilantism and the weaponisation of mediated visibility

Daniel Trottier, dan.trottier@gmail.com, Erasmus University Rotterdam

In 2013, Gary Cleary hanged himself in Leicestershire after being pursued by Letzgo Hunting, an online group that exposes suspected paedophiles. Likewise, in 2015 Walter James Palmer faced global outrage including countless death threats after being identified as the killer of a beloved lion in Zimbabwe. These examples signal an emerging practice whereby citizen use of ubiquitous and domesticated media technologies enable a parallel form of criminal justice. Digital vigilantism is a process where citizens are collectively offended by other citizen activity, and coordinate retaliation on mobile devices and social platforms. The offending acts range from mild breaches of social protocol to terrorist acts and participation in riots. The vigilantism includes, but is not limited to a 'naming and shaming' type of visibility, where the target's home address, work details and other highly sensitive details are published on a public site ('doxxing'), followed by online as well as embodied harassment. Here, weaponised visibility supersedes police intervention as an appropriate response to criminal acts as well as moral outrage. This paper considers digital vigilantism as a user-led assertion of popular sentiment that not only transcends online/offline distinctions as well as distinctions between news media and social media, but also complicates relations of visibility and control between police and the public. In addition to literature on vigilantism and citizen-led violence, this paper draws from surveillance (Lyon 2010, Haggerty and Ericsson 2000) as well as visibility studies (Brighenti 2007; Goldsmith 2010) in order to situate how digital media affordances and cultures inform both the moral and organisational dimensions of digital vigilantism.

Rhetoric of surveillance: a rhetorical understanding of online data use within a Reddit crime-solving sub-forum

David Myles, david.myles@umontreal.ca, Université de Montréal

There has been increasing interest around surveillance practices undertaken by "ordinary" citizens through the use of information and communication technologies in the last few years, most notably in terms of sousveillance (Ali and Mann, 2013), social surveillance (Marwick, 2012), and mundane surveillance (Smith, 2012). The relevance of studying non-organizational surveillance practices (Smith, 2012) lies in the importance of understanding how citizens, like organizations, can also capitalize over online data use within a socio-economical context of informational capitalism (Proulx et al., 2014). In this presentation, we use discourse analysis to understand the surveillance practices undertaken by members of the Reddit Bureau of Investigations (RBI) whose goal is to use "the power of Reddit to solve crimes/mysteries and catch criminals" (Reddit, 2014). RBI members create threads to ask for help in order to solve a crime of which they are often the victim. Using data that spread over a four-month period, our objective is to understand how online data is used by RBI members in a crime-solving capacity. Results show a dual use of online data in RBI members. On one hand, members use online data in a primary objective, that is to solve the various problems to which they are confronted (e.g. track a suspect, identify a vehicle, decrypt messages, etc.). On the other hand, the use of online data also possesses an important rhetorical function. Indeed, we found that online data were used as rhetorical arguments by "victims" to defend the legitimacy of their cases (e.g. to prove their case is valid or that they are not ill-intentioned) and by "investigators" to defend the validity of the hypothesis or solutions they propose. We conclude this presentation by arguing the emergence of a new rhetorical genre, the rhetoric of surveillance, which relies heavily on aptitudes regarding online data tracking and interpretation.

The Uncanny Relationship of Mediatization and Surveillance in Developing Countries

Ilkin Mehrabov, ilkin.mehrabov@kau.se, Karlstad University

Despite being a relatively young field of academic inquiry, mediatization research is already considered to be a prominent theoretical framework for understanding the long term effects of contemporary media saturation. Yet, the empirical research on mediatization conducted so far have focused primarily on Western countries, and was implemented mainly in Europe. There is a growing body of evidence suggesting that especially within the context of developing countries (and also an alarming number of developed ones) media technologies and ICTs are increasingly being used for control over information - together with the heavy surveillance of dissidents and activists. Intertwined merging of mediatized electronic communication with the processes of digitalization; and

convergence of various media forms (shortly called the meta-process of mediatization) inevitably leads to increase in the possibilities of their monitoring - and as the recent revelations of the NSA contractor Edward Snowden and the whistle blower organization WikiLeaks about the global pervasive state surveillance conducted by US and European intelligence agencies in close cooperation with a number of private companies clearly showed, transforms the society into the 'surveillance society' (Lyon, 2001). Thus, in line with Stig Hjarvard's detection that whether the "mediatization has positive or negative consequences cannot be determined in general terms; it is a concrete, analytical question that needs to be addressed in terms of specific contexts, where the influence of specific media over certain institutions is gauged" (2008, p. 114) this presentation aims to focus upon the negative consequences of mediatization and its relationship to increased public and private surveillance with a study on Azerbaijan - where mediatization process is promoted by the modernization upgrades of telecommunications and mobile telephony infrastructure through a number of foreign aids and grants, provided by international organizations and NGOs for the purposes of adjustment towards the governing European and global standards.

Identity and Migration

Surveillance and the 'sub-ject': Examples from the airport

Gabriel Bartl, gabriel.bartl@fu-berlin.de, Freie Universität Berlin

The rise of surveillance points to the question if western societies are really ruled by citizens in a democratic sense or if specific mechanisms – like individualism (Schroer 2001), consumerism (Bauman & Lyon 2013), complexity (Geis 2012), and invisibility (Bellanova 2015) – express the opposite. In the latter perspective the subject is considered as a 'sub-ject' in the narrower sense of the word meaning that autonomous action is nearly fictional, especially in the reflexive modernity (Beck 1986) where different kinds of dislimitations and interdependencies produce unintended side-effects that stand in contrast to the original motives of action. All those processes together block resistance against surveillance that can only be observed on a comparatively low level. In this respect, security measures and surveillance technologies at airports – as representation of failed symbolic politics (Bonß 2012) – can serve as an interesting case example for the study of social, cultural, political, and economical processes hinted at above. The airport as microcosm for

social developments particularly reveals the paradoxes and ambivalences that characterize individual action and organizational structures or political decisions at the same time. Besides, the airport is a place where architecture and atmosphere are coordinated in a specific manner in order to produce unquestionable discipline (Leese 2015).Under this perspective this contribution focuses on the empirical results of a survey that was conducted in 2014 at Airport Berlin-Schönefeld with 1.067 flight passengers. Additionally to analyzing distributions of the data, multivariate methods were used, for example, to shed light on the relationship between different forms of trust and the individual assessment of security measures. As the questionnaire was available in German and English, country-specific differences can be observed with regard to German and British travelers and their attitudes towards CCTV, the potential misuse of the data collected or their trust in modern surveillance technologies.

Between Assimilation & Security: Ethnic surveillance practices and the making of the "Greek Subversive"

Katherine Pendakis, kpendaki@uwo.ca, King's College

During the Greek Junta, between 1967 and 1974, thousands of political migrants arrived in Toronto and Montreal. Joining a diasporic community still polarized by the civil war of the late 1940s, these newcomers created an anti-dictatorship movement that would become consequential for Greek politics in the decades ahead. This article reflects on the practices of knowledge production underpinning constructions of the Greek migrant: One emerging from the social scientific community's interviews and surveys in pursuit of cultural assimilation; the other emerging from the RCMP's record-keeping and surveillance practices in the name of national security. I argue that while sociologists were representing Greek immigrants in a manner that stripped subjects of political agency and political genealogies, the security forces were constructing a starkly opposed profile of the "Greek subversive." I offer here a first-time treatment of RCMP files on this group as well as a critical re-reading of immigration studies from the late 1960s to the early 1980s.

Assessing the societal impact of border crossing technology

Carmela Occhipinti, carmen@eticasconsulting.com, Eticas Research & Consulting

Nowadays, we are experiencing the increased application of emerging technologies for surveillance purposes, requiring recourse to automatic, intelligent, fast and interoperable solutions, designed to gather and analyse all the relevant information. Most of that information can be classified as – even sensitive - personal information (e.g. personal document numbers, biometric parameters, information on nationality, etc.). Consequently, developers of such technologies face highly issues on ethics and other societal concerns related to privacy, social relationships or discrimination just to name a few. This presentation will report the case of EBC4EU, an FP7 European project on Automated Border Control (ABC) gates, experimenting with a legal, social and ethical impact assessment as a tool for defining the legal, social and ethical boundaries that need to be taken into account when designing, developing and validating border management systems.

Borders

Eurodac, changes and transformations before and during the current refugee crisis

Vasilis Vlassis, vavl@itu.dk, IT University of Copenhagen

In light of the refugee crisis, this paper discusses the political discourse around the launch and recast of the Eurodac. The Eurodac is a large scale ICT system used in the scope of EU migration policy as a tool to implement the Dublin convention. The latter dictates that every asylum seeker may apply for asylum to one member-state only, that state being responsible for his/hers application. In order to prevent the practice of double-dipping (applying for asylum in different countries under different identities), all asylum seekers and migrants without documents are fingerprinted and their fingerprints stored in the Eurodac database. The Eurodac is neither controversy-free nor an absolutely stabilized system. Even before launch, the Eurodac's scope was expanded from asylum seekers to migrants without documents. Throughout its existence, the use of fingerprinting, with all criminal connotations it embodies, forensic use has become an issue of discussion. A paper from the Eurodac Supervision Coordination Group states that diverse tactics and methods have been deployed by different state's authorities in cases of failure to provide readable fingerprints, varying from detention to allowance cuts . Finally, since June 2015, the Eurodac database is available to Europol and national police

forces “only in specific cases, under specific circumstances and under strict conditions”,which consists a major shift from the systems’ initial declared purposes. This paper aims to examine and discuss the coincidence of the first period of forensic use of the Eurodac database and the current refugee crisis. How informed are the asylum seekers about the use of their data when they are fingerprinted? How does the fingerprinting procedure affect the migration flows through the points of entrance? What effect was there upon the fingerprinting process the temporary inactiveness of the Dublin convention in the fall of 2015?

‘Big Data at the Border’

Gemma Galdon Clavell, gemma@eticasconsulting.com, Eticas Research & Consulting

Since 9/11, airports and border crossing areas have become critical infrastructures and, some may say, states of exception. The fear that mass transport systems such as planes will be used to conduct terrorist attacks, or that potential terrorists or foreign nationals may abuse their freedom of movement, be it for criminal or other purposes, has permeated the political agenda and guided policy and technology decisions. Moreover, in the aftermath of acts of terror, governments have looked to technology to identify solutions and mitigate risks: full body scanners after the failed bombing of a flight Amsterdam-Detroit in 2010 or Passenger Name Records (PNR) after the recent Paris shootings. At the EU level, a ‘Smart Borders’ package is currently being discussed, including a Registered Traveller Programme (RTP) to facilitate border crossing for pre-approved third-country nationals, an Entry-Exit System to identify over stayers, and an amendment to the Schengen Borders code. It is expected that the automation of border crossing using biometric border gates can both speed up the process and provide increased security by facilitating a quick validation and identification of each traveller. By crossing different databases, it is hoped that red flags will be raised and identify travellers with suspicious travel patterns, diets, behaviour or record, for instance. While database integration is not yet happening at border crossings, much of the security assumptions of this policy initiative relies on the capacity of the technology to identify that which escapes the human eye by getting together and analysing large amounts of data. It is the promise of a border-crossing big data system that underpins the attempts to automate border control. While the European Commission has published reports on the technical and cost aspects of the Smart Border package, several things still require a close look in order to assess the true implications of securing borders through improved data processing, mining and matching. At the end of the day, citizenship is defined and put to the test at the border, and therefore our democratic systems, our definition of citizenship and our relationship to the ‘other’ are both captured and defined in our border crossing procedures

and technologies. The methodology of this paper is based on legal, sociological and anthropological desk research and the work carried out in the EU 7th Framework Programme project 'Automated Border Gates for Europe' (ABC4EU), involving technological companies, police forces and border guards from across Europe. The paper identifies the current and planned status of algorithmic decision-making at border crossings in the EU (databases, public and private data holders, data management chain, transnational collaboration, etc.), and looks at the workings of pre-registered traveller programmes in different EU countries to compare their data-mining mechanisms and levels of algorithmic decision-making, as well as the interaction between data-informed decisions and observation.

Immigration Probation: Legal Liminality, Conditionality and Multi-Scalar Social Sorting

David Moffette, david.moffette@uottawa.ca, Department of Criminology, University of Ottawa

Probationary periods exist in the immigration and citizenship legislations of various countries and the expression is commonly used if not in the laws themselves, at least in the media coverage of these laws. And yet, the literature on the topic is limited and hardly engages in any theorizing of this dimension of immigration governance. In this paper, I outline key dimensions of what I've previously called the "governing of immigration through probation in Spain" (Moffette 2014) and further conceptualize immigration probation in a way that I hope can be useful to those who work on this phenomenon in other contexts. I devised the notion of immigration probation to capture the spatial, temporal and jurisdictional rescaling of borderwork that informs Spanish immigration governance, as well as the continuous multi-dimensional and multi-actor assessment of conditions of desirability that it enables. Ultimately, I argue that the rescaling of borderwork and the ongoing assessment of performance all contribute to creating a probationary period during which—and space where—the ultimate decision to include or exclude is suspended, and yet made and unmade continuously through the ongoing practices of a multiplicity of actors dispersed across space and time and participating in a multi-scalar process of monitoring and social sorting.

State

The French Surveillance State

Valentina Bartolucci, bartoluc@di.unipi.it, University of Pisa

French current counter-terrorism framework relies on extensive societal surveillance in a way that is unique in Europe. While this early warning preventive approach has proven to be a fairly successful in containing the threat of terrorism, it raises questions about unintended consequences for the entire society. In the aftermath of the 2015 Charlie Hebdo massacre new provisions have passed allowing for the use of mass surveillance tolls to tap cell phones, read emails, and force Internet providers to scan customers' Internet use (such as keywords used and sites visited) for the purposes of counter-terrorism with almost no oversight from the judiciary. The new bill sparked protests from international human rights bodies, human rights activists, lawyers, judges, tech companies, and trade unions who claimed it would legalize highly intrusive surveillance methods threatening individual freedom and privacy. This paper seeks to critically evaluate the effects that the recently revised French counter-terrorism strategy can have on its citizens in terms of human rights protection and the ensuring of freedoms. The final aim is to reflect, through the French case-study, on how new discourses and practices of surveillance interact with citizenship, the social context and, crucially, if they are compatible with democracy itself.

Specifics of surveillance in post-communist context

Martin Kovanic, martin.kovanic@uniba.sk, Comenius University

The way individual perceives, responds and reacts towards surveillance depends on the specific surveillance culture of the country. The post-communist area, with its specific legacy of communist surveillance and autocratic control, has its characteristics that influence the attitudes of citizens towards contemporary surveillance. Communist surveillance was characterized by a centrality of file-based surveillance, existence of a wide net of secret police collaborators and an attempt at creation of a transparent citizen. The purpose of this paper is to test how these legacies influence the citizen attitudes towards contemporary surveillance. In the academic literature, there are a number of theoretical explanations which link the functioning of contemporary surveillance with the legacies of authoritarian surveillance – such as mistrust towards public filing surveillance explanation (Samatas

2004, 2014), some of which are specific for the post-communist context – such as fear of crime hypothesis (Los 2002) and support for technological surveillance argument (Svenonius et al. 2014) The aim of this paper is to test these theoretical explanations with empirical data. The main sources of the data are surveys conducted through the PRISMS project and European Social Survey data.

Surveillance in New Europe: The Case of Slovakia

Erik Lastic, erik.lastic@uniba.sk, Comenius University, Dep. of Political Science

The paper's objective is to investigate drivers behind the development and use of surveillance systems on national level in Slovakia and their impact on governance, transparency and accountability. It argues that the recent widespread introduction of national surveillance systems is driven primarily by availability of EU structural funds and political opportunity for clientelism.

Intelligence

Collecting traces, building narratives : Intelligence services and their uses of technologies

Laurent Bonelli, laurent.bonelli@u-paris10.fr, Université Paris Ouest Nanterre

When it comes to anticipating terrorism, do recent technological advancements fundamentally change the modus operandi of intelligence services? Recent scholarship has focused on the new modes of reasoning brought about by 'hi-tech' forms analysis such as data mining, graph visualization and the algorithmic treatment of big data. While this communication recognizes the increasing influence of these techniques, it argues they should not overshadow much more low-tech modalities through which a large part of counterterrorism work takes place. Low-tech counter-terrorism, based on qualitative methods and conjectural reasoning, still matters. Drawing on the case of French domestic intelligence services and based on qualitative interviews, observations and declassified documents, this communication shows that the practices of security professionals, rooted in traditional institutional habituses developed over time, are largely in continuity with previous 'low-tech' forms of police work. In a context in which the uses of digital security technologies have generated discussions about politics and ethics, this article suggests that traditional techniques of

intelligence gathering and processing therefore still merit a great amount of attention. This communication is part of a French research program (Uses of Technologies for Communications Surveillance - UTIC), coordinated by Didier Bigo and myself.

5eyes+ under scrutiny: open season on the personal data of the foreigner?

Elspeth Guild, elspeth.guild@conflits.org, Queen Mary University of London

Didier Bigo, didier.bigo.conflits@gmail.com, Sciences Po

The 5eyes+ countries, first created by an exchange of intelligence among the USA, UK, Australia, Canada and New Zealand (now much enlarged to include 14 countries) has developed beyond the interests of the intelligence community. Interior ministries have begun extensive use of the data exchange system to share information on foreigners which they collect in the context of border, immigration and asylum procedures. While the US constitution requires the US to have formal agreements with other countries which permit this the other (original 5eyes) do not and the personal data exchange takes place according to so-called protocols. This paper will examine the human right to respect for privacy from the perspective of the differentiation between the entitlement to privacy of the citizen vis-a-vis his or her state and that of the foreigner whose personal data appears largely unprotected. Proposed panel with Didier Bigo, Laurent Bonelli, Felix Treguer.

5eyes+ under scrutiny : the visibilisation of the transnational flows of sensitive information by the guild of the transatlantic SIGINT agencies and their private partners.

Didier Bigo, didier.bigo.conflits@gmail.com, Sciences Po

Elspeth Guild, elspeth.guild@conflits.org, Queen Mary University of London

The paper will discuss the practices of the SIGINT agencies working in the so-called 5 EYES + network by doing first a socio-genesis of the type of exchange of information they have shared from the second world war, and by remembering the role of Echelon before the generalisation of Internet. I will in a first part contend that the development of this intrusive practices of large scale surveillance is a natural development of technology and I will also refute that it is a reaction to September 11 2001 and an effect of counterterrorism logic. In the second part I will analyse the paradoxical effects that a transnational acquisition of data based on the circulation worldwide of data of citizen of other countries has on the justification by national security imperatives. This paper is part of a research

project in France called UTIC that analyses the modalities of surveillance, intelligence, espionage, and compliance. Proposed panel: with Laurent Bonelli, Felix Treguer, Elspeth Guild, Didier Bigo

From Deep State Illegality to Law of the Land: The Case of Internet Surveillance in France

Félix Tréguer, felix.treguer@sciencespo.fr, Sciences Po

Taking France as a case-study, the paper reflects on the ongoing legalization strategies pursued by liberal states to secure the Internet surveillance programs operated by their domestic and foreign intelligence agencies amid "post-Snowden contention". Following the path to legalization prior and after the Snowden disclosures of 2013, the paper shows how these leaks helped mobilize civil society groups against the extra-judicial surveillance of Internet communications, a policy area which hitherto had been overlooked by French human rights advocacy. It also points to the dilemma that post-Snowden contention created for governments. On the one hand, the disclosures helped document the growing gap between the existing legal framework and actual surveillance practices, exposing them to litigation and thereby reinforcing the rationale for legalization. But on the other hand, they made such a legislative reform politically risky and unpredictable. In France, policymakers navigated these constraints through a careful mix of distinction strategies, silence, and securitization. After the Paris attacks of January 2015 and a hasty discussion in Parliament, they finally managed to pass the 2015 Intelligence Act. In turn, this reform points to the paradoxical effect of post-Snowden contention: French law now provides clear rules authorizing large-scale surveillance, to a degree of detail that was hard to imagine just a few years ago.

Politics

Voter Relationship Management, the Surveillance of the Electorate and Political Culture

Colin Bennett, cjb@uvic.ca, University of Victoria

Recent presidential elections in the United States have raised to public attention the general question of how political parties and candidates process and analyze personal data on individual voters. An incomplete summary of these techniques incudes: extensive “voter management” databases;

widespread use of personal data purchased from data brokerage firms; extensive use of robo-calling and robo-texting; smart-phone apps that allow door-to-door canvassers instant access to voter histories; extensive uses of social media that allows for peer pressure or "targeted sharing"; and integrated campaign "toolkits" for website development, social media strategies, and political messaging. These techniques have permitted the "micro-targeting" of online and offline messages to more precisely defined categories of voters, especially in marginal states and districts. The range and sophistication of techniques in the US are staggering and unique, and obviously facilitated by the absence of any general data protection law that applies to such data, as well as to a First Amendment that provides robust protections for freedom of communication and association. And of course, these practices are facilitated by a permissive campaign financing system that generally places no restrictions on how much money individual candidates may spend on their election campaigns, or how much they may raise from individuals, groups or corporations. However, there is evidence that parties in other countries are drawing lessons from the American experience, and that similar techniques are gradually entering the politics of other countries. To the extent that "micro-targeting" techniques are entering the election campaigns of other democratic countries, they will have significant implications for privacy laws and for the data protection authorities (DPAs), as well as for electoral and democratic institutions. This paper builds upon my previous research into the privacy implications of these new campaigning practices, an interest that begun with a report to the Privacy Commissioner of Canada on Canadian Federal Political Parties and Privacy Protection in 2012. In this analysis, I investigate the relationship between the spread of voter surveillance practices and political culture. It is often asserted that acceptance of surveillance is related to broader questions of trust in the political system, a theoretical issue that has long been of interest to political scientists. It has been asserted that the stronger protections for data related to 'political affiliation' in European privacy law are explained by cultural factors, and more recent memories of authoritarian rule. But these connections are nuanced and variable, and require more detailed scholarly analysis. This paper attempts to offer that analysis.

"Plenty to Hide": Resistance to Surveillance as a Political Action

Mickey Zar, malmalka@gmail.com, Tel Aviv University

Although resisters have a clear rhetorical interest in classifying resistance to surveillance as civil disobedience or conscientious dissent, the adaptation of those terms to cyberspace raises some grave analytical concerns. Modern jurisprudence tends to frame obedience issues in a sovereign-

versus-citizen context, but it no longer captures the nature of multi-targeted, borderless, covert electronic disobedience. That hybrid nature of resistance calls for revision in the theory of obedience to the law. Legal theory should adapt to current practices of resistance to surveillance and to electronic resistance in general. The proposed talk focuses on one of the difficulties this adaptation might face: the tension between self-interest, traditionally categorizing criminal motivation, and public-interest, traditionally categorizing political motivation. I argue that no form of resistance can be actualized without being hidden from unwanted gaze and scrutiny, at least to some degree and for some stretch of time. In that respect, resistance to surveillance is a prerequisite for all other forms of resistance, and is thus essential to a vibrant public realm. Moreover, social resistance depends also on the participating individual's ability to acquire political agency; since privacy is a dialectic process of self-borders regulation, and since control over those regulation processes is crucial for identity formation and maintenance, defending privacy by resisting surveillance is also a prerequisite for self-determination. Hence, in order to acquire political agency one must have access to a surveillance-free environment. Although legal frameworks tend to acknowledge the importance of defending self-determination processes, they simultaneously tend to ignore the crucial role pervasive surveillance plays in disturbing, suspending and even destroying those processes. Imperative for reconsidering this legal drawback is acknowledging the political nature of resistance to surveillance, even when done individually, in everyday practices such as giving wrong personal details online or using Tor browser.

The Common Gaze: Surveillance, Social Justice and the Common Good.

Eric Stoddart, es61@st-andrews.ac.uk, University of St Andrews

This paper aims to examine mass surveillance in the light of the Common Good, with a view to interrogating the impact of monitoring and sorting upon social justice. It will take the Common Good as a heuristic concept rather than as a substantive, content-filled vision (or visions). In this sense, the Common Good is a style of dialogical engagement between multiple – often diverse, even contradictory, notions of what is good for a community. It will be argued, using the UK as an example, that surveillance is implicated in distortions of the Common Good. First, this is by way of contributing to, although not being the sole cause of, misrepresentations of already-marginalised and denigrated groups of people (e.g., those claiming social security benefits, or immigrants). Second, surveillance has a chilling effect on public debate that is vital to the Common Good in this heuristic sense. This

paper will also explore the irony of surveillance offering a means to expose discrimination and misrepresentation as well as surveillance possibly protecting the public space in which debate may take place. The relationship of surveillance to the Common Good will be presented as an ambivalent one. Consideration will be given to how this approach of discussing surveillance from the perspective of the Common Good might offer saliency, and critical traction, as a rallying-point – perhaps more so than do appeals to privacy. It is surveillance in the form of the Common Gaze that poses acute challenges to developing social justice.

Computer Network Exploitation, Pluralized Surveillance, and Democratic Governance

Adam Molnar, adam.molnar@deakin.edu.au, Deakin University

Erik Zouave, erik.zouave@outlook.com, Citizen Lab, University of Toronto

Governments in Canada, France, Australia, and the United Kingdom (among many others) are undergoing some of the most sweeping changes to anti terrorism legislation since 9/11. The revised laws furnish law enforcement and security intelligence with expanded powers in the 'policing of cyberspace'. More specifically, many of the powers contained in the legislation allow authorities to conduct Computer Network Exploitation (CNE) to further enhance state monitoring, perform equipment interference, and control digital communications in domestic and international jurisdictions. The private sector is indispensable to the 'policing of cyberspace'. Government access to privately stored communications has become a routine dimension of contemporary law enforcement practices. It is now reported that over 60 countries worldwide use privately contracted 'cybertools' and spyware suites for surveillance both domestically and internationally. However, the centralized role of the private sector in developing spyware tools for targeted hacking remains relatively underexamined in the academic literature. In this paper, we examine public-private assemblages as a defining characteristic of CNE operations in both liberal democratic and authoritarian regimes. The development of public-private assemblages in CNE operations signals further transformation within a 'pluralized' field of security and policing provisions as it relates to private sector involvement in state-sanctioned surveillance and information controls. These assemblages give rise to new configurations of institutions, practices, and security governance that redraw boundaries of political authority and challenge the democratic accountability that is required to uphold human rights, privacy, and social justice.

Ubiquitous computing – increasing engagement of private companies in governmental surveillance

Adrian Haase, adrian.haase@hiig.de, Humboldt-Universität zu Berlin

Emma Peters, emma.peters@hiig.de, Humboldt-Universität zu Berlin

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.

Drones

When drones blink

Heidi Herzogenrath-Amelung, h.herzogenrathamelung@westminster.ac.uk, University of Westminster

When a piece of technology is 'on the blink', it isn't working correctly, its proper functioning is interrupted. Seeing has long been a metaphor for surveillance – hence it seems fitting that drones, employed by the military for surveillance and counter-terrorism purposes are referred to in these terms. However, like the human eye, they do not offer continuous and all-encompassing visual record, rather, there is a moment when they 'blink': when one drone needs to be replaced by another. For the military, this moment of quasi-literal darkness represents a challenge because surveillance is interrupted (The Intercept 2015). This contribution seeks to investigate this moment of darkness as a positive possibility for resistance, drawing on concepts from philosophy of technology. This field has so far contributed very little to the project of understanding ubiquitous surveillance, but I would argue that the account of technology given by the German philosopher Martin Heidegger is worth engaging with. In his words "[e]verything functions. That is precisely what is uncanny" (Heidegger 1993 [1966]). Functioning is precisely the basis on which we engage with technology, an ontological quality which Heidegger calls 'readiness-to-hand'. It is what foregrounds the utility of technological objects, and obscures potential negative consequences. When technologies break down however and their proper functioning is interrupted, technologies emerge as as "obstinate", "obtrusive" and "conspicuous" (Heidegger 2008:37). This paper probes the possibilities that emerge from these ruptures in what, under normal circumstances, is a seamlessly functioning informational matrix, drawing on the example of drone surveillance and other techniques constituted by the "surveillance-industrial complex" (Fuchs 2013).

Big data, drone data: Privacy and ethical impacts of the intersection between big data and civil drone deployments

Rachel Finn, rachel.finn@trilateralresearch.com, Trilateral Research & Consulting
Anna Donovan, anna.donovan@trilateralresearch.com, Trilateral Research & Consulting

The use of drones for civil purposes is becoming more and more popular and associated with a growing list of potential applications. Drones are not only becoming smaller, lighter and easier to

control, they are also integrating numerous different types of sensors. Given their growing capabilities and their multiple applications, the privacy and data protection issues associated with drones are also expanding. In addition, these growing capabilities have led some commentators to identify data collected via drones as a key growth area for "big data" (Wigan & Clarke 2013). Like drones, big data is also an expanding emerging technology area where regulators have struggled to keep pace with technological capabilities. However, where big data analytics involve the processing of information either directly or indirectly about people, these techniques also generate significant potential privacy and ethical infringements. Specifically, boyd and Crawford argue, "Big Data is seen as a troubling manifestation of Big Brother, enabling invasions of privacy, decreased civil freedoms, and increased state and corporate control" (2012, p. 664). This paper argues that the intersections of drones and big data augment the privacy and ethical issues associated with each. To do so, we examine two micro-case studies in big drone data, one focused on crisis informatics (e.g., the use of social media and other data for crisis management), which more obviously integrates personal data and another focused on precision agriculture, which seems, on the surface, to raise few issues. The analysis reveals that both practices raise privacy and ethical issues, and discusses three issues common across both micro-cases studies: issues around identifiability, discrimination and equality and the digital divide.

The Political Economy of Unmanned Aerial Vehicles in Canada: the role of stakeholders and the sociotechnical drone space

Ciara Bracken-Roche, 12rcb2@queensu.ca, Dep't of Sociology, Surveillance Studies Centre, Queen's University

Due to the rapid growth of UAV technologies, their implications as surveillance devices may not be adequately addressed through current regulatory mechanisms as the legal and policy frameworks are playing catch up. Two reasons that contribute to this problem are the stakeholder roles in developing and regulating the technologies, and the new asymmetrical visibilities that these technologies bring about. In order to understand the political economy of UAVs in the Canadian domestic realm, this work contributes to this emerging field of research through examining three interrelated things: regulatory issues, stakeholders and their role, and the asymmetrical visibilities that emerge with drone technologies. Preliminary investigations in Canada also show that those developing UAV technologies are also involved in developing regulations which is problematic due to the lack of external consultation with civil liberties advocates, legal scholars and other academics,

let alone the public, who are concerned about the implications of drones. While the political economy of drones may seem to follow a typical trajectory as a technology emerging from the military to the domestic sphere, the role of drones in the surveillance-industrial complex involves different stakeholders as well as new challenges and implications. It is important to understand a) how these technologies develop as socio-technical systems under the influence of specific kinds of stakeholders and b) what's really different about them from already existing surveillance technologies in order to decide how they should be regulated. A key question for academics and regulators is this: are these technologies are unique as surveillance technologies? How do various groups reinforce or change existing power dynamics around emerging surveillance technologies? These questions are addressed in the Canadian context.

Spatialities of aerial surveillance: A critical study of border control by military drones in Switzerland

Silvana Pedrozo, silvana.pedrozo@unine.ch, University of Neuchâtel

Today a variety of surveillance technologies are increasingly being used by public authorities to observe and control national territories. In Switzerland, this technology has firstly been used for various purposes such as observation, mapping and training missions since the beginning of the twenty-first century. However, military drones are now mainly associated with new military interests and surveillance strategies. Military drones are now commonly used to manage and survey borders and cross-border regions. In this context, military drones imply new geographical, political and security strategies for these actors, which redefine aerial surveillance and control practices on the ground. In this view, the objective of this paper is to explore empirically how contemporary surveillance and control practices through military drones participate in, and affect, the management of Swiss border regions. More specifically, the article, firstly, offers a broad discussion of three interrelated spatial logics that characterize drone surveillance, relating to the fundamentally (1) mobile, (2) vertical and (3) adaptable gaze on space offered by the technology. Secondly, the paper shows how exactly drone surveillance is articulated spatially in the explored case study, and how this affects not only the exercise and spatialities of border control but also the very understanding of the border itself by the involved drone users. The empirical insights from Swiss public authorities relating with the use of military drones in border areas provides access to drone's itineraries and control practices in border areas. The set of empirical data contributes to a deepened understanding of the use of this technology for surveillance in Swiss cross-border regions.

Drone Seduction

Leandro Huerto, leahuert@ucm.es, Goldsmiths, University of London

The goal of this paper is to reposition the ethics of drone warfare and discuss the allure that it has when used for military purposes. It is about the humanization of the target, instead of visualizing it as a convergence of data. There's a big call upon criticizing this technologically deterministic attitude that substitutes personal identity for data as most of the killed targets have been victims. As a direct example and reference I will be using the Drone Papers that were leaked in The Intercept. Drone warfare will be addressed as a counter terrorist strategy in civilian territory so that the public has an understanding what it actually means to be surveilled by air presence. The meaning of warfare shifts completely and there is a lack of morality same as physicality since the offender is not present. Leading to an invulnerability winning situation. I will end the topic by proving that it has been counter productive and creates more counter insurgents or even prospective terrorist as victims are instilled by hate towards the U.S. Furthermore, touching how profoundly democracies are opting for the investment in robotics of war. Ultimately, this strategy of never knowing where the enemy is and being aware that it could attack anytime produces a sense of panopticon where every day civilians feel scrutinized and observed without feeling safe even when they're in their homes. It is time to instill a debate about the morality that the usage of drone warfare entails and be critical about its usage.

Spatialities of surveillance

Francisco Klauser, francisco.klauser@unine.ch, University of Neuchâtel

Theoretical and empirical research has long suggested that surveillance tends not only to relate to specific persons or social groups but also to select, differentiate and manage specific categories of space. However, whilst the importance of space as the locus, object and tool of surveillance has been acknowledged, there has to date been little attempt to bring the existing studies together in order to approach the spatial dimensions of surveillance more fully and rigorously.
The presentation seeks to open up such an endeavour. More specifically, the presentation draws with critical distance upon differing spatial vocabularies to discern the complex ways in which surveillance interacts with space. Hereby, three levels of terminology can be distinguished. The first is the

vocabulary of points, lines and planes, together with derived notions such as nodes, networks and rings. Second is the terminology of Foucauldian 'spatial problems', distinguishing between fixity, enclosure and internal partitioning on the one hand, and flexibility, circulations and openness on the other, and third is that of Sloterdijkian spheres. This tripartite structure is not meant to set apart clearly distinct levels of analysis of the surveillance-space nexus. On the contrary, my aim is to demonstrate that different spatial logics of surveillance, captured through various taxonomies, inform each other, support each other, modify and shape each other, but also conflict with each other in ceaseless reciprocity. In addressing this broad analytical and conceptual problematic, the presentation focuses in particular on examples of visual surveillance through drones and CCTV cameras.

Body cams

Body worn video cameras, policing and surveillance: who is protecting whom?

Anthony Minnaar, aminnaar@unisa.ac.za, University of South Africa

While the wearing of body cameras, as opposed merely to the routine use of dashboard cameras mounted in patrol vehicles, by law enforcement officers, particularly specialised policing units, has been in use for a number of years, a refocus on their use occurred in 2014. This refocus came about after a number of incidents, particularly shooting deaths by police officers, and led to a steep rise in the number of policing agencies, particularly in the USA, purchasing and equipping their officers with so-called 'body worn video cameras'. Conflicting motivations for their increased use were made by, not only law enforcement but also civil society and human rights (privacy) groups. This paper examines those often opposing viewpoints, the motivations of why police officers should start wearing and using them, and issues of public security and protection, as well as the issue of surveillance privacy rights. Among ancillary issues were those of creating a video (surveillance) database of police officer conduct; recording of crime in action; post-crime tracking of offenders but also whether such video surveillance information to be used as digital evidence in any cases of police misconduct. However, in the rush to equip police officers with body cameras there was a noticeable absence of any formal guidelines for their operational use, as well as for surveillance information utilisation. Further complicating factors in their use by law enforcement officers being whether body camera video footage could become part of the public record as evidence in an investigation of an officer-involved death, use-of-force incident

and/or the discharge of a weapon and whether such digital evidence could be used (justification) to charge a police officer for a crime.

The Rise of Body-Worn Video Cameras: A New Surveillance Revolution?

C. William R. Webster, william.webster@stir.ac.uk, University of Stirling

Charles Leleux, charles.leleux@stir.ac.uk, University of Stirling

The use of body-worn video (BWV) in the UK is growing steadily and is being used routinely by public officials in relation to policing, community safety, car parking and in the public transport environment. It is being introduced for a variety of reasons, including, to deter assaults on staff, to provide evidence of incidents and to record interactions between service providers and users. Despite their growing use relatively little is known about the numbers of devices deployed, their technical capability, costs, and governance arrangements, or whether BWV complies with data protection and other legislation. This paper seeks to address this knowledge gap, by providing preliminary evidence about the use of BWV in a number of public service settings in Scotland. It provides a basic overview of the numbers of BWV deployed, their primary purpose, cost, as well as a comparison of data processing arrangements and governance practices, and some of the practical issues associated with the effective deployment of this technology. The widespread use of BWV is becoming normalised in encounters between citizens and public officials and arguably represents a new dimension to citizen-state relations. In the US there have been calls from politicians for police officers to be routinely equipped with BWV, following the deaths of young black males in police custody. The investigation into the police shooting in 2011 of Mark Duggan in the UK, called for 'urgent improvement in the accountability of police operations after it found that a lack of audio or video material made it impossible to know with certainty exactly what happened.' However, the diffusion of BWV has not been accompanied by guidelines governing their use and oversight, and it is apparent that differing approaches to deployment and data management are emerging. It is evident that we currently know very little about the diffusion of BWV.

Policing as (Monitored) Performance: Police Body Cameras, Citizen Video, and New Visibility

Bryce Newell, b.c.newell@uvt.nl, Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University

Body-worn camera (BWC) adoption by police in the United States has placed individual officers in a position of drastically increased (secondary) visibility. As a response to the deepening community mistrust of police and the image management problems spurred by the rise of citizen video, BWCs are changing the very nature of what it means for officers to 'perform' while on-duty (and how officers report their encounters in post-incident reports). Kevin Haggerty has suggested that the ability of the citizenry to watch the powerful represents a major development for surveillance theory, and that the realization by those in power of their own visibility will lead them to "develop a self-interest in the politics of surveillance." The widespread adoption of BWCs by local police departments in the United States, partially as a response to the increasing ubiquity of citizen video, appears to be one such response. However, findings indicate that officers see BWCs as both a defensive response to citizen video as well as something that just makes the 'problem' worse — often at the same time. The recording of non-arrest, 'peace keeping,' activities may subject officers to oversight from a variety of sources that may diminish their ability to 'act alternatively' in situations where they might otherwise have chosen not to, for example, make an arrest. Report writing also becomes a task of aligning narrative and documentary evidence. Consequently, officers must now 'perform' satisfactorily (in the streets and on paper) for a vast audience or risk losing their jobs and at substantial risk of reputational harm. Drawing on findings from empirical research with two police departments in the United States, this study seeks to provide a better understanding of the impact of BWC adoption (and the laws that regulate the use of these devices) on everyday police work.

Police-Worn Body Cameras: Comparing empirical studies in the Netherlands and United States

Bryce Newell, ola.svenonius@sh.se, B.C.Newell@uvt.nl

Tjerk Timan, fredrika.bjorklund@sh.se, t.timan@uvt.nl

After a looming and almost silent introduction in several Western countries over the past decade, recent events have led to the increased adoption of body cameras by police agencies as well as (re)new(ed) media and scholarly attention. These cameras, likely to become standard police equipment in the very near future (if not already), have sparked controversy and raised questions surrounding the purpose and use of their deployment—a controversy that is most visible in the United

States. While often introduced to protect and safeguard on-duty police officers by acting as an objective witness, or to hold officers accountable for misconduct, critics fear the cameras will merely contribute to the swelling state surveillance apparatus and increase citizen visibility vis-à-vis the state. Within the expanding ecosystem of cameras in modern society, including smartphones, CCTV, drones, traditional cameras, and other wearables, police body cameras play a number of complementary and conflicting roles; they collect evidence, exonerate officers, incriminate officers, modify behavior, and do all of these while moving easily between public and private spaces. As with citizen video, body cameras increase the visibility of individual police officers as well as the nature of policing more generally. These developments may lead to changes in how policing is perceived by the public and, potentially, to how policing practices are employed in actual practice. In this paper, we compare two empirical studies of the introduction and use of police-worn body cameras—one conducted with two municipal police departments in Washington State (US), and the second performed in Enschede and Rotterdam (NL). Both studies utilize interviews and participatory observation and, for purposes of this paper, focus on the experiences of police officers as the end-users of these cameras and as actors performing for multiple lenses while they work.

What do Detainees Think of Police Body-Worn Video Cameras?

Emmeline Taylor, emmeline.taylor@anu.edu.au, Australian National University

Body-worn video (BWV) cameras are increasingly being used by Australian frontline police officers. First trialled in Northbridge, Western Australia in 2007, the use of BWV cameras is rapidly growing. Despite significant investment in this technology, very little is known about the impact of BWV cameras on offenders, witnesses, the public, or indeed on police behaviour. The broad objectives of police BWV cameras are to increase transparency and accountability; improve behaviour among police officers and citizens; expedite resolution of citizen complaints or lawsuits against police; improve evidence for arrest and prosecution; and provide opportunities for police training (White 2014). While there is some emerging evidence that the technology can change police behaviour for the better, through reduced use of force, for example, there has to date been no research exploring the perceptions of arrestees. This study reports on findings from interviews with police detainees just after arrest, in four state capitals across Australia.

Citizenship and the Body

Surveillant screens: Biometrics and the hygienic body

Rob Heynen, rob.heynen@gmail.com, York University

This paper seeks to build on work examining the impact of systems of surveillance on bodies, and in particular how those bodies are constituted along lines of race, class, gender, sexuality, and/or disability, with the focus on the role of screens in mediating practices of surveillance and self-surveillance. The paper begins by sketching a brief genealogy of these screen practices, in particular in the deployment of film in the late 19th and early 20th century in emerging biopolitical strategies of individual and social hygiene. Ranging from the work of Frank and Lillian Gilbreth to public hygiene films in early cinema, we find that screen practices did not simply 'represent' bodies; more fundamentally, they rendered bodies as data ripe for intervention and manipulation, with 'hygiene' the lens through which this occurred. These historical contexts provide important contexts for understanding the intensification of biometric regimes in digital neo-liberal hygienic practices. This paper addresses these contemporary practices from two inter-connected directions: those of large-scale biometric systems and of the growing use of 'personal' biometrics. In the first instance I look at scientific texts in the field of biometrics, arguing that the visualization and screening of bodies in such surveillance technologies involve the inscription of 'hygienic' bodies structured again by conceptions of race, class, gender, sexuality, and disability. In the second instance, I examine the development of the 'quantified self' evident in technologies like Fitbit. Here too, albeit in a very different register, surveillance and self-surveillance involves the use of biometric data in the regulation of the body. Where much of the literature in surveillance studies tends to represent these emerging digital technologies as marking a radical break, an historical framing enables us to trace deep historical continuities as well as ruptures in contemporary biometric systems.

Surveillance in harm reduction programming: The case of new electronic documenting and reporting requirements in Toronto, Canada

Adrian Guta, aguta@uottawa.ca, University of Ottawa

Emily van der Meulen, evandermeulen@ryerson.ca, Ryerson University

Zoë Dodd, zoe_dodd@hotmail.com, N/A

Martin French, martin.french@concordia.ca, Concordia University

This presentation will explore a new and contentious trend within community-based harm reduction programs in the form of increasing mechanisms for the surveillance of people who use drugs by service providers, community-based organizations, and public health authorities. Harm reduction is a collection of practices and policies aimed to reduce risks related to consuming drugs (e.g., infections and overdose). In the past decade, harm reduction has become a more accepted strategy in public health in Canada, the USA, UK, western Europe, and Australia in response to growing evidence demonstrating its effectiveness in reducing both individual and social harms associated with drug use. However, the increased formal recognition of harm reduction, including through state funded programs to provide sterile injection and inhalation equipment, and safe spaces to consume drugs, has resulted in tradeoffs for community-based organizations and the users of their services in the form of greater visibility, reporting, and surveillance. Such surveillance is said to improve organizational efficiency and the user experience, but important questions need to be asked about the implications of the data collected. To make sense of these trends we draw on Foucauldian theory and revisit early concerns that harm reduction programs could become biopolitical strategies to govern drugs users. Specifically, we focus on the growing use of “NeoSystems” software in community-based organizations in Toronto, Canada. This computer program collects and stores demographic information about drug users, their substance use preferences, information about tests/diagnoses of blood born infections, and the types and amount of supplies they take at each visit. We offer theoretical and applied critiques of the ways in which NeoSystems, and other similar surveillance technologies, may serve to undermine harm reduction programing by undoing the trust built between organizations and drug users, the ethical implications of the data collected including its use/non-use, and its legal implications.

Consumption

Monitoring, Measuring and Maximizing: Surveilling Citizenship through Consumption Practices

Jason Pridmore, pridmore@eshcc.eur.nl, Erasmus University

This paper focuses on the production of citizenship through the dynamic and iterative processes of consumption and the increasing surveillance of these practices. Though citizenship may be taken as a given in certain contexts, this paper argues that citizenship is something (continually) done and that forms of consumption are a significant means of “doing citizenship”. Drawing from a performative understanding of marketing practices, citizenship can be seen as both described and enacted

through various configurations that can be examined through the concept of surveillance. The surveillance of consumption helps illuminate our understandings of citizenship by highlighting how the visibility and invisibility of citizens are being performed various contexts. It demonstrates the relational production of power dynamics for both the state and the complicity of corporate actors in the process. This paper examines this interconnected relationship between the surveillance of consumption and citizenship through three illustrations. First, the paper focuses on interest of the state in consumptive practices as part of the calculation of particular risks. In this, the mundane activities of citizens become scrutinized for suspicious behaviour and concerns, particularly within financial and travel sectors. Most notably this is connected to the surveillance of consumers in relation to money laundering, organized crime, and passenger records. Second, the paper examines a bit further increasing shifts in the provision of identity. While the state remains the primary arbitrator of identity, increasing this 'official' verification process matters less. Although the state may provide the means for accomplishing identification tasks in some specific circumstances, increasingly private companies serve to verify identity in ways that are unheard of previously. These experiences have led to increased consumer demands for similar functionality within state institutions, perhaps most clearly seen in funded calls regarding the servicing of citizens through new tools for co-creation and collaboration with government (particularly in the European Union). Finally, this paper notes that the means for citizen participation in governmental affairs is increasingly occurring within private forms of (social) media consumption. That is, both political discussions and citizen engagement through and within (social) media have become a key form of engagement – of active rather than passive citizens – however these spaces are subject to a myriad of different modes and technologies of surveillance. These three illustrations reiterate that the intentions and capacities for surveillance in the consumer sphere are inseparable from how citizenship is now 'done'. The visibilities and invisibilities of citizenship now are embedded in this surveillance and the data produced creates new predictive potentials that make certain groups meaningful in terms of citizenship. There are core social, ethical and legal principles that need consideration both for those interested in the changing nature of citizenship and the increasingly blurred boundaries between public and private.

Consuming surveillance. Consumerism and social practices as a new frame for theorising about surveillance

Nils Zurawski, nils.zurawski@uni-hamburg.de, University of Hamburg

How to frame surveillance theoretically beyond panopticism, Deleuzian assemblages or the discourse of social sorting that are so dominant in the literature? With an approach that views

surveillance as an element of consumption beyond the rather banal monitoring of consumption itself, I want to explore and discuss the theoretical implication of such an endeavour. Based on a variety empirical research (loyalty cards, shopping, doping tests and controls, data protection and everyday practices, assessments of digital technology after Snowden) I will outline how surveillance forms part of everyday social practices, becoming such a practices itself. Following Bauman's work on consumerism and the wider notion of consumer capitalism, I will argue that surveillance has become an object of consumption itself, the more so as it is being rendered ambient, pervasive and hence often unrecognisable and therefore acceptable or indeed an object of desire, a commodity as such. This means that surveillance becomes hidden in a sense, that nobody calls it surveillance or monitoring or control anymore, but something else, as it will be embedded in other practices, surveillance is becoming that very practice itself. With such an approach it may be possible to better account for the dynamics of social practices in a consumer capitalism, which is also driven by the ongoing expansion of digitisation of social life and hence society as a whole. I will offer a theoretical account to discuss its further implications and reach for the overall study of surveillance.

Health

Security, Distinction, Markets: Influenza surveillance in Germany and its problematizations

Kevin Hall, hall@em.uni-frankfurt.de, Goethe University Frankfurt, Germany

Nearly 20 years ago David Armstrong (1995) observed "The rise of surveillance medicine". With the outbreaks of highly pathogenic avian influenza H5N1, SARS, pandemic influenza H1N1, MERS-CoV and most recently the outbreaks of Ebola haemorrhagic fever in West Africa the development of surveillance medicine has gained considerable momentum. In the process of visualising outbreaks syndromic surveillance systems partake in the construction of a pandemic threat and claim the authority to represent the possible future threat of disease outbreaks. Recent scholarship has emphasised the contemporary association of (global) public health with security issues (e.g. Elbe, King, Lakoff and Collier). An example for this association is the combination of pandemic preparedness planning with diverse forms of disease surveillance that link pandemic alert levels and the measures to be taken at each level to the detection of the infectious pandemic agent within the

state territory. However, the focus on security issues in scholarship on disease surveillance might have diverted attention away from the micro practices of disease surveillance and its effects on everyday life. In drawing on the example of influenza surveillance in Germany this paper will outline two other problematizations (Rabinow) that lead to the development of this sophisticated syndromic surveillance system before the threat of a pandemic became the single most important reason for disease surveillance. The paper will argue that influenza surveillance sought to answer the question of the actual disease burden of seasonal flu and its impact on the national economy on the one hand, and tried to raise the vaccination rates in the German population on the other hand. By examining how influenza surveillance is conducted the paper draws attention to the processes by which practices of surveillance create, govern, and maintain social order by acting upon how we know and experience the space surrounding us (Zurawski, Lyon).

Desire, risk, and surveillance: New forms of visibility and modes of governing people living with and affected by HIV

Adrian Guta, aguta@uottawa.ca, University of Ottawa
Alex McClelland, mcclelland.alex@gmail.com, Concordia University
Stuart J. Murray, Stuart.Murray@carleton.ca, Carleton University

In this presentation we discuss the implications of new HIV treatment and prevention technologies in the form of HIV 'treatment as prevention' (TasP) and 'Pre-exposure Prophylaxis' (PrEP) in the North American context. TasP is an intervention targeted at people living with HIV, and involves scaling up HIV testing and antiretroviral therapy to improve health outcomes and reduce further transmissions. Meanwhile, PrEP is targeted at people deemed 'at risk' of acquiring HIV and involves prescribing the same HIV antiretroviral therapy—but to prevent infection. Together, they constitute what the US Centers for Disease Control and Prevention have termed "high impact prevention," an approach that uses "combinations of scientifically proven, cost-effective, and scalable interventions targeted to the right populations in the right geographic areas." Gay, bisexual, and other men who have sex with men living in urban centers like San Francisco, New York, Toronto, and Montreal have been targeted through both official public health and community-initiated health promotion messaging. Those living with HIV are urged to start treatment and maintain an undetectable viral load while those at risk of HIV are urged to take control of their health and sexuality by initiating PrEP. While these pharmacological approaches have great promise for increasing access to HIV testing, treatment, and prevention, they have also enabled new forms of medical and public health surveillance that need to

be questioned. Specifically, both TasP and PrEP require greater healthcare utilization and in the case of TasP have legal implications. Drawing on critical insights from Michel Foucault and Robert Esposito, we explore how HIV +/- gay men are engaging in new ways with public health, clinical care providers, and each other in ways that promote their governance within an immunity paradigm.

Quantified Self

In the name of wellbeing: Self-tracking as surveillance

Btihaj Ajana, bajana@aias.au.dk, AIAS

Recently, the use of algorithms, data and metric technologies has invaded many spheres of production, knowledge and expertise. From marketing and advertising to healthcare and bioinformatics, various fields are currently exploring the possible benefits and challenges pertaining to the collection and usage of data for different purposes and contexts. In my presentation I consider the example of the Quantified Self movement and the concept of Health 2.0. I discuss how data-driven techniques of self-tracking are becoming popular solutions in health management at both the individual level and in the wider context of healthcare. While such developments are often considered as positive trends towards self-improvement and health monitoring, they are also raising various ethical issues, some of which relate the intensification of surveillance practices by self and others.

Surveillance and quantified body

Anna M. Potocka, anna.marta.potocka@dekra.com, DEKRA Hochschule für Medien

This contribution identifies and analyses risks of surveillance and data collection in the context of health tracking and quantified-self. An intrinsic characteristic of the postmodern condition we live in are multiple power centres which make us control, reflect and evaluate our-selves and who eloquently seduce us to share all possible information about our-Selves. This lust of control and self-optimisation leads us to self-exploitation and alienates the quantified body from the Self.

The quantified self between 'play' and 'control'

Imge Ozcan, imge.ozcan@vub.ac.be, Vrije Universiteit Brussel

The Quantified Self (QS) technologies which people use to track various metrics related to their bodies and engage in practices of self-care and self-governance are increasingly being integrated into institutional logics. With its emphasis on control and optimization, QS sits comfortably within well-known Foucauldian governmentality themes. Actually what Foucault called "technologies of the self", means through which individuals relate to themselves in certain ways and conduct themselves, takes on a literal meaning in the contemporary self-tracking practices. This paper will briefly introduce QS and will build upon the governmentality literature to address the social and ethical implications of QS technologies and practices. Secondly, it will investigate the playfulness and participation elements associated with these technologies and will explore the surveillance dynamics implied by self-tracking practices. Finally, it will problematize the integration of QS technologies and practices into corporate wellness programs and insurance markets.

Social Media

The Social Media Account as Interface: Platform, Infrastructure & Financial Value

Greg Elmer, elmer.greg@gmail.com, Ryerson

Largely conceived of as free-standing, semi-autonomous properties, social media platforms have thrived on the user-generated content of their individual members. The growth in such user accounts has been closely monitored by media analysts and Wall Street firms looking to define, measure, and attribute economic value for share holders. Yet simultaneously the platform-account has been undermined by social media companies, whether it be in the form of constantly changing End User Agreements, Terms of Service, or Privacy Policies, or through the data-mining and incorporation of non-account holders into social networks, commonly referred to as 'ghost profiling'. Critiques of social media companies, however, largely rest on arguments over the exploitation of users or ongoing privacy violations – both of which invoke the platform-account as the principle interface between user and company. An analysis of Facebook and Google's networked account-infrastructure ("sign-in with

your Facebook account") where user profiles are "ported" across platforms, will show that social media companies' ongoing search for financial value is increasingly located at the interface between platform and account-infrastructure. The paper thus posits a critical framework of social media beyond the individual user and toward the account-infrastructure.

Social Media and Scrutiny: Young adults' perceptions and practices

Justine Gangneux, justinegangneux@gmail.com, College of Social Sciences, The University of Glasgow

This research explores young adults' understandings of social media platforms and how these impact on their personal relationships in their everyday life. Platforms such as Facebook, Instagram or Twitter are framed as a means of enhanced scrutiny in these relationships. Indeed these technologies provide increasing capacities for 'checking', 'scrutinizing,' 'looking up' (Joinson, 2008), and 'searching', potentially leading to a normalisation of such practices. Using in depth qualitative interviews with young adults aged 18-25, the research adopts a critical approach to social media and surveillance (van Dijck, 2013, Fuchs, 2014). by looking at these platforms, neither simply through the framework of empowerment and participation (Albrechtslund, 2008, Koskela 2006), nor solely through the framework of risks and safety (e.g. social control, top-down commercial and state surveillance). My research focuses on these technologies a means of social sorting and, of normalisation of scrutiny and checking practices in peer relationships. It is embedded in a wider economical context of assimilation of work and play, increasing insecurity and, promotion of the entrepreneurial and reflective self (Sennett, 1998, Giddens, 1991, Kelly, 2006, Standing 2011). Using Bourdieu's theory (1984, 1998), this paper investigates the place of surveillance, information gathering and checking practices in young adults' media practices and understandings but also importantly looks at the shifting perceptions, discourses and legitimacies of these practices in everyday life (Andrejevic, 2007, Jansson, 2012, Marwick, 2012). Indeed according to Andrejevic (2007), continuous and normalised interactions with surveillance processes make possible the emergence of a 'culture of peer-to-peer monitoring that mimics and amplifies top–down forms of commercial and political surveillance' (Ibid. : 213). This has been coined as a 'surveillance creep' (Trottier, 2012), i.e. the spread of surveillance practices from one context to another, consequently leading to a normalisation of these practices. This paper, in particular, examines whether these increased capacities for scrutiny, enabled by these technologies, amplify or/and normalise such practices in young adults' everyday social relations.

Use of Social Media at Work: A New Form of Employee Voice?

Peter Holland, peter.holland@buseco.monash.edu.au, Monash University

Brian K Cooper, Monash University

Rob Hecker, Monash University

Social Media such as Twitter and Facebook were originally designed as electronic social platforms that have in the 21st century morphed into some of the most powerful communication tools both inside and outside the workplace. However, whilst much of the focus has been on the potential negative and destructive (dark) aspects of social media at work, less attention has been given to the harnessing of social media in a human resource management (HRM) context. This paper examines the relationships between social media, job satisfaction and age using data from the Australian Electronic Workplace Survey (AEWS). We find that the level of job satisfaction is a key factor in the desire to use social media in the workplace. Our findings are consistent with the proposition that social media use at work is a response to job dissatisfaction and can be interpreted as a new form of voice behaviour, especially among younger workers. Although we find evidence social media is being used as a channel for frustrated younger employees to vent in response to dissatisfaction at work., we conclude that social media has the capacity to flatten the organisational hierarchy of voice channels at work as it gives everyone connected the opportunity to have equal input and management an immediate understanding of workplace issues and perspectives.

Constitutive Surveillance and Social Media

Ryan Tippet, ryan.tippet@gmail.com, University of Otago

The default and implicit assumption in much surveillance studies literature locates social media arising apart from its surveillance society context, and, correspondingly, sees surveillance as an independent process that invades social media. This relational perspective linking social media and surveillance is one of 'appropriation', and presupposes social media and surveillance to be structurally distinct entities. I demonstrate in this paper how the perspective of such a relational gap can be reoriented towards one of 'constitutive' surveillance. A constitutive perspective of surveillance, formulated with reference to Foucauldian theory, sees the generalised logics of visibility, knowability, hierarchy, and control not as exterior to social media, but central to it – constitutive of it. Constitutive

surveillance suggests that social media has, from its origins, been a set of technologies governed by surveillance, rather than an unadulterated medium colonised by surveillance in the post-bust emergence of 'Web 2.0' platforms. Social media is constituted by surveillance, and indissociable from the surveillance society context out of which it emerges. In order to formulate the concept of constitutive surveillance, I examine the idea of surveillance as a strategy of power in a Foucauldian sense – that is, a micro-physics that determines the relations and vectors of the objects within it. Surveillance constitutes social media to the extent that surveillance power necessitates a maximisation of visibility and rationalisation, and thus produces in social media an ideal machine for that pursuit. A social media platform such as Facebook, I argue, is constituted by surveillance of three interrelated forms – political, economic, and lateral peer surveillance – while oppositional practices are still constituted in part by surveillance through their self-definition as opposed to, yet paradigmatically within, surveillance power.

Mapping intersectionality: investigating new methodologies for studies in surveillance and social media

Jacquelyn Burkell, jburkell@uwo.ca, University of Western Ontario

Sarah Heath, sheath@uottawa.ca, University of Ottawa

'The eQuality Project' seeks to understand young people's experiences with various forms of surveillance (e.g. peer to peer, panoptic, synoptic), discrimination, and equality online. Such work requires an intersectional lens to fully understand the impact on youth who occupy a position at the intersection of various marginalized identities (e.g., gender, race, sexual orientation, etc.). In particular, intersectionality implies and requires a comparative approach to identify differences in experiences and conceptions across those who occupy different social positions. Concept mapping and Q-sorting, two research approaches that use quantitative methods to explore subjective opinions and perspectives, present two possible strategies to meet these research needs. In the current context, these methods support exploration of the ways in which diverse groups of young people conceptualize constructs such as privacy, while at the same time allowing identification and analysis of differences across groups. This paper will present a critical examination of the literature on concept mapping and Q-sorting along with preliminary findings that uses these techniques to examine gender differences in their perceptions of the personal/private nature of one form of social network information: personal photographs. Our results will examine whether young men and young women share views on the types and sensitivity of the kinds of personal photographs typically posted in

online social profiles. The critical analysis and results will be discussed in relation to the question of whether these research strategies support the goals and principles of an intersectional approach to privacy and surveillance, and therefore provide an appropriate method for studying youth experiences of surveillance and social media through an intersectional lens.

#LayingLow: (In)Visibility on Social Media and Violence in the 'Hood'

Marta-Marika Urbanik, urbanik@ualberta.ca, University of Alberta
Kevin D. Haggerty, khaggert@ualberta.ca, University of Alberta

One of the most controversial components of the increasing reach of, and dependence on, various social media platforms has been rampant concerns about visibility, user privacy and potential consequences of user indiscretion as related to online presence. Much of this emphasis has centered upon consequences directly related to the effects of increased publicity on brand reputation, employment, and online harassment. While all users of social media are subject to its potential dangers, little is know about social media use can affect the lives of specific groups, namely those who occupy a marginalized position in society, and consequently, how this position may exacerbate the potential dangers of social media usage. More specifically, little is known about how social media enables surveillance for a different purpose, namely for the purpose of locating individuals for the purpose of enacting violence. Based upon 140 interviews, and over 400 hours of ethnographic observation in Canada's oldest and largest social housing complex- Regent Park,- our research has revealed the ways that participants maintain a presence on social media platforms such as Instagram and SnapChat, whilst at the same time consciously thwarting their visibility- specifically, their whereabouts- in order to reduce the potential of violent victimization. These intricate strategies range from avoidance of specific social media platforms all together, to more careful management of 'real time' social media, to strategies of 'late' posting, in order to hinder potential assailant's knowledge of individual's locations. As such, we propose that users understand the ways that social media platforms are used as a means of surveillance, specifically for the purpose of enacting violence, which affects the extent of visibility of certain groups on social media, revealing yet another site of their marginalization.

Resisting the Academic Social Media Surveillance State

Sava Saheli Singh, sava@nyu.edu, NYU

Being an academic today more often than not includes being an academic online. Blogging, tweeting, maintaining profiles on sites like academia.edu – this academic digital labor is an expected part of the service to knowledge. And for good reason: for many academics, being online increases visibility and aids in the dissemination of scholarly work. But it also means being exposed to very direct surveillance by institutions, peers, students, and others, which can affect academic life in a number of ways. Who you are and the amount of social capital you command have very real implications on your professional and personal life as performed through social media platforms like Twitter. My research focuses on the academic and scholarly use of Twitter and the impact that this platform has had on what it means to be an academic, from academic freedom to academic FOMO (fear of missing out). Recent cases like Saida Grundy and Steven Salaita serve as stark lessons in the negative impact of social media surveillance. But academics are increasingly encouraged to be on Twitter – sometimes with specific guidelines from their institutions on accepted forms on behavior and engagement. This public performance of academic identity then becomes a complex balance between authenticity, self-promotion, and toeing the line, in order to appease a shifting audience of those who surveil, while unwittingly and ironically participating in the very surveillance that we pander to, that platforms like Twitter encourage by their very design. In this paper I will address the interplay between academic identity and surveillance on Twitter. I will examine how this affects the professional and personal lives of academics, their communities, and the scholarly work they produce, while they submit to or attempt to resist the academic social media surveillance state.

Privacy

The luxury of leading a private life: A privilege for the lucky few?

Julia Maria Mönig, post@juliamaria-moenig.de, DFG Research Training Group “Privacy”: Forms, Functions, Transformations at the University of Passau

When my health insurance gives me a discount because my smartwatch has told them that I've been doing my sit-ups, what's wrong with that? When a journalist spends over 2,200 US-Dollars and 'countless hours' in one year to protect her data, where's the problem? Let's say it is what the respective companies do with our data and what they know about us: our privacy. Privacy, historically as well as in examples like the above-mentioned, sometimes appears to be a privilege that only

applies to those who are wealthy, healthy and educated enough to profit from its advantages. This also fits together with the observation that surveillance has affected the less privileged more than the privileged members of society. However, with smart technologies the opportunities to track peoples movements and their whole lifes increases. In this talk three central issues will be explored: First, historical examples that private affairs of the members of the upper class have been better protected than the data and the personal spheres of those with less money and less power. Second, it will be tried to disprove the talks own hypothesis by asking whether today persons with more money do undergo more — potential — privacy violations since they have more money and therefore more possibilities to use technical gadgets and smart technologies which might by privacy infringing. Third, the paradox between privacy as a right for everyone and a privilege for the 'lucky few' will be tackled. The theses will be reconciled by differentiating between different types and dimensions of privacy and arising questions of solidarity, equality and (a-)symmetries of power will be posed.

The Construction of Privacy, Publicity and Citizenship in Canadian Search and Seizure Jurisprudence

Valerie Steeves, vsteeves@rogers.com, University of Ottawa

At least since the introduction of video cameras in the 1980s, Canadian courts have struggled to balance the citizen's right to privacy with the state's interest in using information technologies to investigate crimes. Over the next 30 years, as new technologies emerged, legislators tended to expand police powers by enacting special provisions to allow police to use the latest information tools to hit the market (e.g. general warrants to allow video surveillance, production orders to access computer data, lawful access provisions to provide access to metadata). Courts have been slow to constrain this expansion, typically relying upon an artificial distinction between bodily or territorial privacy (which attracts a high level of protection) from information about bodies or places (which attracts a lower level of protection). Twenty-first century surveillance, which is both ubiquitous and mundane, complicates this distinction, in three interrelated ways. First, the traditional sharp lines between private spaces (which are protected from warrantless access on the part of the state) and public spaces (which are not) are blurred when police link location data from a variety of sources (cell phones, social media, video traces) with data continuously collected and shared by smart environments and surveillance drones. Second, although police are typically not allowed to search the body or the home without a warrant, data that emanate from those sources are increasingly collected by corporations and later voluntarily shared with police. Big data promises to exponentially

increase this flow as sensors embedded in our bodies, homes and electronic devices routinely collect information about our communications, interactions, bodies and attitudes/preferences. Third, big data logic may overwhelm the legal mechanisms we rely upon to ensure that the police cannot overreach their authority and upset the democratic balance of power between state and citizen; whereas judicial logic examines individual pieces of information about individuals accused of crimes and examines their investigatory meaning ex post facto, big data preemptively collects all data, however mundane, from all citizens on an ongoing basis and analyzes it for unknown patterns that may or may not prove to be criminal, in effect reversing the presumption of innocence. This paper will examine Canadian jurisprudence on search and seizure in cases where information technologies are implicated (e.g. cell tower dumps to identify all persons within an area in which a crime occurred, access to metadata) to identify the legal reasoning that supports the expansion or constraint of police surveillance powers, and compare and contrast this jurisprudence with older cases that articulate the need for democratic limits of police surveillance in non-networked spaces. In particular, it will map the ways in which courts have constructed the meaning of privacy, publicity and citizenship over time and explore the extent to which current legal discourses are developing (or failing to develop) a robust understanding of the role that privacy plays in democratic governance.

The spread of the right to informational self-determination, a response to surveillance

Kamel Ajji, kamelajji@gmail.com, Université Paris 2 Panthéon Assas

When it comes to the regulation of surveillance mechanisms, debates, protests and decisions turn around privacy. This right is takes roots in the right to informational self-determination. The latter, developed by the German Federal Constitutional Court in its 1983 decision (Volkszählungsurteil), is the “capacity of the individual to determine in principle the disclosure and use of his/her personal data”. It entitles the individual to decide which of his/her informations can or can't be collected and/or processed. The FCC based this right on both human dignity (art. 1§1 of the Basic Law) and personality rights (art. 2§1 BL). The individual can influence the sphere's creation. The former refers to the liberal principle of being left alone by the authorities. It's about keeping the authorities out the sphere. The FCC distinguishes between, on the one hand, storage and access to data, and, on the other, direct and indirect use of data by the authorities. Further, the Court replaces the individual in the whole society to underline the global risks of surveillance. In this contribution, we will analyze the spread of this right, especially in France. The State's Council (Conseil d'Etat), in its 2014 report,

"Digital technology and fundamental rights", pleads for its adoption. The authority distinguishes ISD and data property rights for users, arguing that the latter doesn't fit the need of both users and authorities. The recent Intelligence Act (Loi sur le Renseignement, 2015) seems to put this concept aside. The recent attacks in Paris prompted politicians to pledge for more data surveillance, relying on emergency, emotions, people's fear and safety expectations. These legitimate ends can't be ignored, but still, we need to think about the balance our societies must find to preserve rights and freedoms. How could this right be adjusted to security requirements? Proportionality isn't heard the same way in France and in Germany. ISD, as defined by the German FCC, encompasses the communication in itself (the message) and its context (when, who, where). In other words, the collection of metadata is breaching the Basic Law. Is ISD already outdated? How do French Conseil d'Etat intend to apply it in France? On what ground? Which procedures could be developed? Do the European Courts (ECHR, and ECJ) recognize this right? We will try to answer those questions, and many more, in this contribution.

"Your Bodies are Temples of the Holy Spirit". A Theological Approach to Surveillance Society and the Transcendence and Transformation of Religious Communities

Susanne Wigorts Yngvesson, susanne.wigorts.yngvesson@ths.se, Stockholm School of Theology

Synagogues, Churches and Mosques are targets and subjects in surveillance society. This is a well-known fact round the world, even in low-criminal countries such as Sweden. Religious buildings are the target for violence, which have created an increased need for surveillance personnel and technologies such as CCTV-cameras and id-control. These surveillance practices makes the buildings hyper-visible (Baudrillard) in a secular surrounding, and design the inner logic of the religious community as a space for security and threat. From a political perspective some religious communities and buildings can be surveilled for hosting suspects and therefor surveilled through the governmental regime (Foucault; Butler). Hence, some surveillance technologies are installed by initiative from the communities for safety, while others are used for the sake of public and governmental security. In this paper some arguments about the practical and political reasons for surveillance of religious buildings and "bodies" will be presented. The analysis concerns the consequences of surveillance practices in some theological and philosophical perspectives, i.e. friction surfaces of theological and political discourses. The narrative within all the Abrahamic religions includes belief in God as monotheistic, and humans as Imago Dei (the image of God). Further, from a transcendent point of view nothing can be revealed from God. As a parallel to the

visibility from God's perspective, the general politics of surveillance aims towards a transparent society. The managing makes humans products/creations of surveillance in a liquid society (Bauman; Lyon; Schneier). Humans become bound to necessity, as Imago Techne, a design of information and control. Hence, the aim of this paper is to a) analyze how the different discourses can be compared as objects and users of surveillance, and b) analyze how the discourses can be used as critique towards surveillance of religious buildings and communities in Sweden.

Internet service providers as privacy custodians

Mike Zajko, zajko@ualberta.ca, University of Alberta

This paper examines the role of internet service providers (ISPs) as guardians of personal information and protectors of privacy, with a particular focus on how telecom companies in Canada have historically negotiated these responsibilities. ISPs have formal legal obligations to safeguard the privacy of their subscribers and the communications passing through their networks. However, there are differences in how ISPs operating in the same jurisdiction interpret these obligations, or engage with state and non-state actors that seek access to personal information and data flows. Communications intermediaries have long been expected to act as privacy custodians by their users, while simultaneously being subject to pressures to collect, utilize, and disclose personal information. As service providers gain custody over increasing volumes of highly-sensitive information, their importance as privacy custodians has been brought into starker relief and explicitly recognized as a core responsibility. However, commitments to privacy stewardship are often neutralized through contradictory legal obligations (such as mandated surveillance access) and are recurrently threatened by commercial pressures to monetize personal information. I argue that struggles over the responsibilities of our privacy custodians are some of the most consequential aspects of ongoing debates over surveillance and privacy. Users often express skepticism about the commitment of their service providers to privacy, and companies wishing to cement their reputation as privacy custodians must be willing to take an active stand against the various pressures that seek to pry into the most sensitive of information flows.

Privacy: a matter of control or access, and why it matters

Kevin Macnish, K.N.J.Macnish@leeds.ac.uk, University of Leeds

There has been a debate regarding whether privacy is a matter of control or access for some time. This debate has taken on a greater sense of urgency in light of the revelations made by Edward Snowden in 2013 regarding the collection of swathes of data from the internet by signals intelligence agencies such as NSA and GCHQ. The nature of this collection is such that if the control account is correct then there has been a significant invasion of people's privacy. If, though, the access account is correct then, while there has still been an invasion of privacy, this is less egregious. Furthermore, while the privacy lobby has tended to adopt the control account, the governments of the UK and US adopt the access account. This has often resulted in a lack of effective communication between the two parties. I argue that the control account of privacy is incorrect. However, the consequences of this are not that seizing control of my information is therefore unproblematic. I argue that the control account, while mistaken, is plausible for two reasons. The first is that a loss of control over my information entails harm to the same rights and interests that privacy protects. The second is that a loss of control over my information increases the risk that my information will be accessed and that my privacy will therefore be violated. Taken together, the result of these two reasons could be that a loss of control is more harmful than a violation of privacy. As such, in disputing the ethics of signals intelligence bulk collection, framing the debate in terms of a privacy violation could be less effective than alternative approaches.

"An ounce of privacy" - Comparing privacy attitudes in the United Kingdom and the Netherlands

Anouk Mols, anoukevelienmols@gmail.com, Erasmus University Rotterdam

Open curtains and a careless attitude. Dutch citizens are perceived as taking an indifferent stance towards privacy. In contrast, the United Kingdom staged heated debates about privacy concerning ID cards, CCTV and data collection by the NSA and GCHQ. Snowden's NSA revelations reaffirmed that citizens have little or no control over how, when, and where their personal data is used by whom and for which goal in our current data-driven era. The opaque nature of governmental and consumer surveillance presses the need for insights in how individuals think about data collection methods that infringe their personal and public lives. Recent survey results showed that UK citizens are more concerned about their privacy and control of their personal information than Dutch citizens. Drawing upon a notion of privacy as a social issue, this study transcends the individual level and explores how

(relations between) individual, societal and governmental entities play a role in privacy attitudes in public debate about Snowden's first revelations in the United Kingdom and the Netherlands. The research design consists of an inductive frame analysis of online and offline reactions, including both journalistic and user-generated content, and a descriptive quantitative analysis. The in-depth analysis enables the interpretation of voices within the debates and provides an overview of the distribution of privacy attitudes. Preliminary results showed how privacy activists, politicians, users and academics play an important role in the debates. They provide the basis for privacy attitudes ranging from a careless notion of 'nothing to hide' to the digital defeatist 'privacy is dead'-frame. In addition, a comparison is offered between privacy attitudes in the two countries to see whether the Dutch are as aloof as claimed and if their reactions contrast yet another heated debate in the UK.

Bodies as Risky Resources: Japan's colonial ID system and its implication today

Midori Ogasawara, himawarimido@nifty.com, Queen's University

Surveillance systems today are massive but highly individualistic, identifying the population as individuals, accumulating data on an individual basis across spheres, and tracking individual movements physically and virtually. In such an expansion of personal data, enabled by networked databases, biometrics is seen as the ultimate identifier of the 'truth'. The body is targeted as the final evidence of self and the original source of data in today's worldwide techno-political complex. Although the individualizing characteristics visibly proliferated after the "war on terror" since 2001, the demand to govern individual bodies can be traced back to modern institutions: the nation-state, bureaucracy, capitalism and colonialism (Weber 1946, Giddens 1981, Marx 1976, Foucault 1977, Lyon 2009). Among them, colonial times and places tend to be original laboratories where bodily schemes generate. Fingerprinting was invented in British India (Cole 2001). Fingerprinted ID cards were implemented to identify the civil population and track individual movements in Manchuria in Northeast China, too, under Japan's occupation in the 1920s–1945. This paper examines ID techniques in occupied Manchuria as a root of present ID systems, and discusses the implications of their focus on individual bodies. The Manchurian techniques were crystallized in the rapid construction of modern capitalism and nation-states, under contending Japanese imperialism and Chinese nationalism, in order to mobilize the population for production and war. The Manchurian ID systems performed dual tasks: preempting potential rebellion among the local Chinese and using them as cheap labour power for the empire. Their bodies were reduced to risks but profitable resources, by the individualizing ID system.

Those practices can be framed as a technique of biopower (Foucault 1978), the state of exception (Agamben 1998), and necropolitics (Mbembe 2003). Japan's Manchurian ID systems remark the contemporary feature of surveillance that manages to force and cajole oppositions to work in unison and to make them serve the same reality in concert (Bauman and Lyon 2013).

Big Data

Performing and negotiating family tracking

Anders Albrechtslund, alb@dac.au.dk, Aarhus University
Lise Lotte Beck Andersen, liselotteba@gmail.com, Aarhus University
Louise Nørgaard Glud, imvlng@dac.au.dk, Aarhus University

This paper explores and analyses the use of tracking technologies in the sphere of intimacy, particularly in matters of family life. In recent years, a wide variety of devices, apps and services have become available for family use, such as tools for parents to track their children's activities and home camera devices to capture and document moments and events in the private space of the family. This leads to discussions about parental overprotection opposite child independence as well as questions of trust and security in family relations (Fotel and Thomsen, 2004; Rooney, 2010). The use of tracking technologies in families implicate negotiations about the boundaries of trust and intimacy in parent-child relations which can lead to strategies of resistance or modification. Tracking is surveillance in accordance with the commonly used definition of a practice characterized by "focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction" (Lyon, 2007, p. 14). As a mode of surveillance, tracking entails issues concerning agency, control and power relations, but at the same time, it is a practice performed by and for individuals in the intimate context of their private lives. The paper reports from a qualitative inquiry which is particularly focused on generational relations, including interviews with children aged 10-14 and their parents. The purpose is to investigate why tracking technologies are adopted by families and how these technologies potentially change the relation between parents and children. The case study addresses the following questions: What motivates the use of tracking technologies in families, and how does the use transform the relations between parent and child? How are the boundaries and possibilities of tracking negotiated and managed in families? References: Fotel, T., & Thomsen, T. U. (2004). The Surveillance of Children's Mobility. Surveillance & Society, 1(4), 535-554.Lyon, D. (2007). Surveillance Studies: an overview. Cambridge, UK; Malden, MA: Polity.Rooney,

T. (2010). Trusting Children: How do surveillance technologies alter a child's experience of trust, risk and responsibility? Surveillance & Society, 7(3/4), 344–355.

Attitudes Towards Surveillance in Everyday Life. Google Big Data in Cross National Perspective

Anna Franczak, aniafranczak@hotmail.com, Polish Academy of Science

Scandal with PRISM global data surveillance program exposed in 2013 was a confirmation that we live in a surveillance culture which has become an integral part of our life. The explosion of the internet would not be possible without us - we often share our personal data and opinions, we communicate with others. In the real world we have got use to CCTV cameras. We can't escape this reality but we should be aware of it. Are we? In our everyday life are we interested in data privacy? Do we want to learn how to protect our data? What is the law in this matter? These are the questions I would like to answer. To estimate public interest for the purpose of the project I used Google tools which allow to check what people search for. I focused on 4 topics: (1)Edward Snowden and WikiLeaks; (2) Digital safety (what is internet safety, data protection); (3) Looking for advice (how to protect my data online, cyber security training); (4) Law and regulations (information security policy). I analyzed the data from the last 3 years, in 179 countries using over 6000 search terms in local languages. Since June 2013 until now, month by month, I followed a number of searches for each of these topics to estimate our interest. When do we search the most? Now or right after publication about PRISM? How this trend is changing over time? Do we search more often about it? What are the differences? In which country is the interest about surveillance and data protection largest and in which smallest? If we add variables like GDP and Democracy Index – are there any interesting correlations? During the conference I would like to present the full results of this study in cross-national perspective.

Big Data Surveillance: What's 'new'?

David Lyon, lyond@queensu.ca, Queen's University

Big Data (BD) did not appear as a new set of practices but as a concatenation, an amalgamation of previous practices. Surveillance of many kinds has for a decade and more been influenced by the discrete practices that are now referred to collectively as BD. So it is important to ask where BD came from, what the real differences made by BD are, and whether the use of BD practices is likely to add

up to a genuinely qualitative change in the ways that surveillance is conducted. This paper first explores the origins of BD in enabling digital dataveillance, government-corporate linkages, the appearance of BD practices in most major surveillance trends and their connections with the emerging surveillance culture. Second, key areas of changed practice are identified, in modes of data capture and analysis, a suggestion made that deeper changes in surveillance practices are discernible. Third, the question of qualitative change is addressed in both empirical and theoretical ways. Are there potentially permanent differences of approach that might be explained in terms of a structural shift in the distribution of authoritative and allocative resources and a challenge to the knowledgeability of everyday actors – the subjects of surveillance? In terms of its origins BD surveillance is hardly a 'new' phenomenon but because of the ways that it is being developed, it may well have distinctively 'new' impacts in terms of its consequences.

Big Data in the Education Arena: 21st Century Student Sorting and Tracking

Priscilla Regan, pregan@gmu.edu, George Mason University
Jolene Jesse, jjesse@nsf.gov, National Science Foundation
Elsa Talat Khwaja, ekhwaja@masonlive.gmu.edu, George Mason University

Student tracking in the 1950's, especially in heterogeneous societies such as the United States, resulted in classrooms that were often divided by race, ethnicity, gender and class. Such tracking was glaringly obvious to parents, students, teachers and administrators – and thus their implications and wisdom became subjects of policy and social debate. The student tracking that is occurring in 2015 is hidden from view as it takes place behind computer screens in the different educational programs that different students are exposed to – based on how big data applications have evaluated their likely learning profile. One of the arenas in which big data applications is presently being aggressively marketed is education, not only at the college level but perhaps even more so at the elementary and secondary level. As educators and administrators focus more attention on the effectiveness of teaching techniques, student learning outcomes, and budgetary constraints, new applications facilitated by and facilitating big data are being developed and implemented in many countries. The benefits of big data applications include more sophisticated analyses of student learning and testing, more personalized learning, more effective delivery of educational materials, improved assessment, and more responsiveness to student needs. On the downside big data applications and products raise the possibility of discrimination as a result of profiling and tracking of students, as well as uses of student information for a wider range of purposes. This paper seeks to

first analyze the big data educational market – who are the key players, are they primarily country-specific firms or global firms: how are the benefits and downsides of big data applications being framed in marketing materials; what types of educational institutions, levels, and/or subjects are being targeted. Second, the paper will explore whether educators and/or civil society groups are responding to big data educational innovations – what discourse has resulted; what themes are being voiced and by whom; in what venues are discussion taking place. Third, the paper is particularly interested in discussions about whether and how categories such as race, gender, ethnicity, and class, as well as their intersections, are affected by big data applications in education – and what the implications of this are, particularly for children in their early educational years where opportunities for future learning may be critically shaped. Finally, the paper will close with a comparison of the policy and social debates in the 1950s about educational tracking and those of the 20'teens.

CCTV

Visual surveillance in the City of London: from the top down and the bottom up

Kevin Biderman, kevin.biderman@network.rca.ac.uk, United Kingdom

This paper outlines contemporary developments in visual surveillance practice within the City of London. It highlights current trends, which strategically utilise subjective identity as a means of governance and control. It argues that surveillance tactics are being embedded in and outsourced to the individual as a 'standard' behaviour. In doing so contemporary modes of governmentality, as Foucault claimed, utilise the population through the "apparatuses of security" (Foucault 1991:102). I focus on the way in which, as Cruikshank's states, "government works through […] the subjectivity of its citizens" (1999:69). Here we see key roles outsourced to the local community; on one hand as a means to police, on the other to aid the functioning of a shrinking state and the further inclusion of the private sector. Lines are blurred between counter terrorism and crime control; the operations of the state and private industry. To explore this, I examine the recent progression of visual surveillance arrangements in the City, instigated by the police. The current movement towards mobile operations such as Project Servator attempts to isolate and exclude 'hostile' identities while at the same time incorporating other individuals into a collaboration with the police. Through a conflation of terrorism, ordinary crime and protest, authorities utilise means validated by fear of a drastic attack to support

all their operations. I closely examine promotional materials for Project Servator to see how a unity between the public and the police is being fused for such aims. Subsequently, the way in which the City Police categorise the London Occupy group is explored to illustrate how Project Servator might disable regulatory agency from the bottom up. Finally, I utilise Nicholas Mirzoeff's (2011) exploration of visuality and the right to look in order to uncover how repressive structural arrangements might be subverted.

Unsettling the city: critically examining the effect of CCTV beyond order

Caitlin Overington, caitlin.overington@unimelb.edu.au, University of Melbourne

Surveillance technologies have become deeply embedded in everyday life. Expanding beyond top-down approaches to governance, studies now turn to focus on these increasingly complex and adaptive practices. Alongside (and in relation to) these technological evolutions and entwined assemblages though, the role of surveillance in policing practices must continue to be interrogated. Closed-circuit television cameras are firmly fixed within the architecture of many modern cities. While often disappearing into the background of the urban environment in the everyday context, CCTV footage continues to amplify when this everyday-ness is ruptured by deviance. Images recorded by these fixed cameras are carefully sutured together – either by police or news media – and are released as part of a narrative of making sense of crime in the city. This crime image, through its composition and imperfect framing of the space, has a multitude of effects. Through a selection of case studies and interviews, this paper will draw out how a relatively banal surveillance technology continues to have a profound impact on the everyday. This will be framed within relational visibility. Firstly, this paper will critically engage with the normative assumption that expanding CCTV networks will result in expanding spaces of order. Particularly when recording at night, the image created by these cameras instead projects the city as unsettled, with ever-present elements of darkness and risk that cannot be mitigated with more cameras. In other words, CCTV images expand the scene of the crime spatially and temporally through its circulation. This leads to the paper's second assertion, which argues how this visibly 'imperfect' functionality of CCTV works more broadly in favour of expanding surveillance practices. Post-criminal events, CCTV returns to the background of the city, but not before contributing indirectly to the narrative of surveillance in general as simultaneously critical to, yet not invasive of, the everyday.

Usage of Surveillance Cameras at home and Culture of Surveillance

Ozge Girgin, 14og@queensu.ca, Queen's University

CCTV cameras in the public places is a common phenomenon for various reasons in many locations around the world. The use of security cameras within home has also been a growing business. The voluntarily installed cameras at home in various locations by the homeowners are used primarily among other factors to monitor the property and the employees or specifically to monitor and control the behaviours of the nanny or the babysitter. The increased installation of surveillance cameras in the houses with the possibility of remote monitoring can be seen as an extension of the culture of surveillance and integration of surveillance within the private lives. The domestic usage of cameras embodies the monitoring of the self in addition to the surveillance of the employee. The monitoring of the nanny, on the other hand, reinforces the unequal power relationship embedded in the work process. Moreover, the usage of the cameras entails the supposed consent of the involuntary participants of the surveillance. The camera usage in domestic places and private spheres can be linked to normalization of everyday life surveillance practices. In drawing on the culture of fear highlighted by David Lyon and Michel Foucault's of Panopticon, this paper discusses the use of surveillance cameras in private spaces as an implication of culture of surveillance. I argue that entering a house with cameras implies giving consent to be under surveillance similar to and as an extension of being under the gaze of the CCTV cameras in public places.

Gated Communities: A Statistical Scrutiny of Existing Hypotheses

Pawel Waszkiewicz, p.waszkiewicz@wpia.uw.edu.pl, University of Warsaw
Fredrika Björklund, fredrika.bjorklund@sh.se, Södertörns högskola
Ola Svenonius, ola.svenonius@sh.se, Södertörn University

Gated communities are housing areas that have been enclosed in one way or another, typically involving heavy use of surveillance technology (see Addington & Rennison, 2015). Such areas were first described in the USA and South Africa in the late 80s and early 90s (McKenzie, 1994; Blakely & Snyder, 1997). Since then they has been focal points of several research projects in different regions of the world (Low, 2003; Glasze, 2003). There is a significant number of publications covering the increasing number of gated communities in Central and Eastern Europe (CEE) after democratization of formerly communist societies (Bodnar & Molnar, 2009). In the post-communist context, a general lack of trust, the increasing socio-economic polarization, fear of crime and the existential insecurity

created in the democratization process have been forwarded as potential explanations for the rapid expansion of gated communities (Hirt & Petrovic, 2010). However, these hypotheses derive mostly from qualitative studies and yet await more quantitative scrutiny. To this end, the project Like Fish in Water: Surveillance in Post-Communist Societies commissioned field work in Estonia, Poland, and Serbia during Winter 2014-15. A representative and probabilistic sample of 1000 respondents from each country were interviewed face-to-face on matters of trust, security, surveillance and a range of contextual aspoects, among others gated communities. The Like Fish in Water survey enables us to evaluate existing hypotheses on the expansion of gated communities in the CEE from a statistical perspective. The aim of this paper is thus to scrutinize existing hypotheses and develop the existing theorizing on gated communities derived from the literature, with particular focus on matters of trust.

NSA & Ethics

The Five Eyes Alliance after Snowden

Felicity Ruby, Frub3005@uni.sydney.edu.au, Sydney University

Edward Snowden's revelations have made the US National Security Agency (NSA) a household name. A less well known term is ‘Five Eyes,’ an abbreviation of the term ‘AUS/CAN/NZ/UK/US EYES ONLY,’ which refers to the intelligence collection and sharing arrangement between the USA, UK, Australia, New Zealand, and Canada, which had its beginnings in 1946. Only with the facilities and intelligence institutions of the Five Eyes partners combined — that is, infrastructure, labour, shared understanding and practices, knowledge, information, and data built out over 70 years — can the NSA conduct global mass surveillance. Coalitions of organisations have formed in Five Eyes countries to protest mass surveillance: Stop Watching Us in the US, Don’t Spy on Us in the UK, Citizens not Suspects in Australia, Oasis from Surveillance in New Zealand and Protect our Privacy in Canada. While activists, journalists, technologists, academics and isolated policy makers are fighting for a digital world free of spying, intrusion and authoritarian invasions of privacy, many governments are making retrospectively legalizing what Edward Snowden exposed ignoring international law on the right to privacy, freedom of expression and association. These groups from Five Eyes countries feel both an opportunity and responsibility to paint a clearer target on the problems their governments have imposed on the world and the future of the Internet, stating, “While our governments have wrought enormous damage to human rights and international law, they also

demonstrate the utility of coordination and joint strategies." This paper will bring the history and role of the Five Eyes intelligence alliance to discussion of a surveillance society and examine resistance strategies adopted by social movements.

Would You Do What Snowden Did? An International Study of University Students' Reactions to Snowden's Actions and Revelations

Andrew Adams, aaa@meiji.ac.jp, Centre for Business Information Ethics, Meiji University
Kiyoshi Murata, kmurata@meiji.ac.jp, Meiji University
Yasunori Fukuta, yasufkt@meiji.ac.jp, School of Commerce, Meiji University
Yohko Orito, orito.yohko.mm@ehime-u.ac.jp, Ehime University
Ana Maria Lara Palma, amlara@ubu.es, University of Burgos

The series of revelations made by Edward Snowden revelations starting on 5th June 2013 exposed a true picture of state surveillance or, more precisely, surveillance conducted by an industrial-government complex in the democratic nations. His revelations have attracted heavy doses of both praise and censure; whereas some have positively evaluated his deed as an act of valour to protect democracy against the tyranny of the state, others have criticised him as a traitor to his country that have been preoccupied with responses to the threat of terrorism since the 9.11 attacks. Indeed, the US government filed charges of spying against him on 21st June, and he is forced to live in exile in Moscow. He said that only the American people could decide whether sacrificing his life was worth it by their response. The Pew Research Foundation found in a survey that although Americans are deeply split on whether Snowden's actions served or harmed the public interest, that younger groups regarded his actions as more beneficial than harmful although older groups tended to be more critical of his actions. Inspired by the Pew Research Foundation's surveys, an international group of academics led by the authors of this paper conducted surveys on young people (students at their universities) about their attitudes to privacy online, and the actions of Bradley/Chelsea Manning and Edward Snowden in separate and different modes of grand leaks. This survey has been deployed in China, Germany, Japan, Mexico, New Zealand, Spain, Sweden and Taiwan. (Mis)Trusted parties, willingness to emulate Snowden (in the US or at home) and the source of their knowledge of Snowden's information were all covered in the survey, which revealed some stark and (the authors think) interesting international differences.

Philosophy, epistemology and ethics of surveillance

Giampaolo Ghilardi, g.ghilardi@unicampus.it, Università Campus Biomedico Roma

Roberto Setola, r.setola@unicampus.it, Università Campus Biomedico Roma

Surveillance is the action to pay close and sustained attention to another person or to a specific object. This paper provides an overview of its history and philosophy by focusing on the formal feature that makes surveillance what it is. In particular, we will analyze at what conditions an act of observation becomes an act of surveillance. From Bentham's Panopticon to Orwell's Big Brother, there has always been a preference accorded to the sense of sight in the action of "overseeing". However, new generation Biometrics has caused a paradigm shift, which will be analyzed in light of what Foucault names "punishment of bodiless reality". We will also consider the epistemology of surveillance. Specifically, we will focus on the shift from the old surveillance model, according to which forbidden signs were meant to warn the person under surveillance about a possible dangerous reaction from the overseer, such as a watch dog or a soldier, to new models, aiming to inform the person under surveillance about being watched overtime. We will look into the origins of modern surveillance techniques and their link to the raise of modern science, specifically to the connection between quantitative knowledge and the concept of control. We will argue that Surveillance is not an ethically neutral concept and that its ethical nature depends on at least three different elements: object, intentions, and circumstances. Finally, we will point out how ethics, far from being an obstacle, could be a useful tool to achieve the same goal that surveillance pursues.

Data Activism

Data activism as an emerging epistemic culture within civil society

Stefania Milan, s.milan@uva.nl, University of Amsterdam

As massive data collection progressively invades all spheres of contemporary society, citizens grow increasingly aware of the critical role of information as the new fabric of social life. This awareness triggers new forms of civic engagement and political action that I have termed 'data activism'. Data activism indicates the series of social practices that at different levels, in different forms, and from different points of departure are concerned with a critical approach to big data, and massive data collection in particular. Data activists address massive data collection as both a challenge to individual rights, and a novel set of opportunities for social change. They appropriate technological innovation, and software in particular, for political or social change purposes. This (relatively) new empirical phenomenon emerges at the intersection of the social and technological dimensions of human action. It rises from the open-source and hacker movements, but overcomes their elitist character to increasingly involve ordinary users, thus signaling a change in perspective towards massive data collection emerging within civil society. It concerns both individuals and groups, and operates at different territorial levels, from local to transnational. This theoretical paper explores the notion data activism as a heuristic tool to think politically about big data, and massive data collection in particular. It offers a conceptual map to approach grassroots engagement with data from an interdisciplinary perspective, combining political sociology, science and technology studies, international relations and critical security studies. Finally, it outlines a typology of data activism, and positions it in the contemporary social movement ecology.

'Information disorder was not enough': Radical Technology Collectives as sustainable anti-surveillance efforts

Maxigas, maxigas@anargeek.net, UOC/IN3

This presentation addresses questions of temporality, trust and resistance in the context of the contemporary surveillance landscape from the point of view of radical technology collectives. Radical technology collectives provide online infrastructures such as mailboxes and websites to mostly local activist groups and individuals. The empirical material draws from experiences of five different

decade(s) old collectives. Positioned at a passage point where social conflicts are translated between political, technical and legal matters, they have earned the trust of activists in Brasil, France, Germany, Italy and the Netherlands. Most were founded during the alter-globalisation cycle of struggles and played an important part in the movement. Unlike many other activist groups such as Indymedia, they have continued to be active until now. Moreover, they persisted in the new strategic context of increased (awareness of) mass surveillance. In contrast, some commercial providers with a similar profile such as Lavabit (that Edward Snowden used) and Silent Circle (associated with security expert Bruce Schneider) closed down in 2013 in response to pressure from authorities. I compare the resistance of RTCs to surveillance with those of commercial providers as well as with the proposals of hackers for decentralised technological solutions. The latter (such as Twister or GNU Social) distribute trust in a different way that may be harder to assemble and sustain. Finally, I note that decentralised and commercial solutions are argued for largely in terms of technological determinism (a flight to a universal future) while the rhetorics of RTCs have more affinity with ideas of social construction (proven track record in a community).

Instrumentalising Risk to Conduct Surveillance and Defend Against it: the Risk Calculation Practices of Cybersecurity Actors and Human Rights Defenders

Becky Kazansky, r.kazansky@uva.nl, University of Amsterdam

This paper critically examines the increased use of 'threat modeling' practices to predict and mitigate potential data security risks. In doing so, it traces socially prevalent rationalities around risk and risk calculation, as these rationalities are re-inscribed and re-produced within data security assemblages. Threat models are used among seemingly counterposed security actors such as governmental national security officials, developers of Free Libre Open Source security and privacy enhancing technologies, and human rights defenders. Threat models take the form of text-based specifications for the design of secure systems; as discursive frames for societal messaging of security threats and risks; and as programmed and enacted elements of information infrastructure. Through threat models, security actors anticipate the most costly and likely 'data risks,' rationalise protective and offensive measures in response to risks, formulate risk registers and risk communications for the public, and design and implement new sociotechnical information infrastructure. This paper argues that the rise of threat modeling practices is indicative of an 'anticipatory turn' in cyber, information, and ICT/data security, borne out of a broader preoccupation with quantifying and

forecasting risk. Further, it argues that the growing prevalence of threat modeling practices figures into a militarised feedback loop of increasing societal concern with security, referred to in critical security studies literature as a process of 'securitisation'. Of specific concern are the effects which securitisation may have upon the work of human rights defenders and civil society actors in how they are able to protect themselves and resist monitoring, surveillance, and massive data collection processes. Do threat modeling practices contribute to the protection of human rights defenders and civil society actors, or instead reproduce the very 'risks' they try to mitigate? The paper draws upon the preliminary findings of a theoretical and empirical PhD research study undertaken at the University of Amsterdam within the ERC-funded DATACTIVE project.

Convergence of moments: the online broadcasting of protests

Lucas Melgaço, lucas.melgaco@vub.ac.be, Vrije Universiteit Brussel

When the first CCTV cameras appeared, many started to fantasize about the image of a constant presence of an agent behind the screens, monitoring one's steps in real time. Reality quickly proved to be very different. Agents did indeed look at screens in control rooms, but video surveillance became more important in investigations using past footage than in real time interventions. However, this situation has transformed with the increasing automation of surveillance processes, as in the case of smart CCTV systems, but also with the emergence of online video broadcasting technologies like Periscope and Meerkat. Without being concretely present in the streets, activists are able to watch and interact with real-time videos broadcasted by other demonstrators, who film these events using smartphones and social media. More than ever before, today, there is what Brazilian geographer Milton Santos called "a convergence of moments," that is to say, the capacity of "sharing" the same moment, instantaneously, but from distance. By analyzing recent cases of protests in Brazil and Belgium, this presentation will reflect upon the use of real-time broadcasting technologies by amateur citizen journalists. Among the examples will be the cases where these sousveillance practices played a role in the protection of protesters against police brutality.

Smart Technologies

Living in a Panopticon City: the Biological-Behavioural-Geographic-Economic-Social-Physical-Medical Complex – People and Places under Dynamic Surveillance

Andelka Phillips, andelka.phillips@law.ox.ac.uk, University of Oxford

I. S. Mian, s.mian@cs.ucl.ac.uk, UCL

Jan Charbonneau, Jan.Charbonneau@utas.edu.au, University of Tasmania

Once upon a time it was possible to keep our stories private. Today, we are no longer in control of our personal stories. Our information is collected, analysed, and shared widely, often without our knowledge. It's 2016, not Orwell's 1984 – or is it? Perhaps we are in fact unknowingly living in Bentham's Panopticon. Let's begin with one person's story. Hilda purchases a direct-to-consumer genetic test but her genomic data – the most personal data she has – is not just for her eyes, it could be shared by the company with or without her knowledge. Her wearable health monitoring technology doesn't just tell her how far she walked, it provides the company with a raft of personal data. Her smart bathroom scales and Internet connected refrigerator not only collect data about her weight or whether she is out of milk, they also transmit information about her dietary intake and weight management, often with pictures. Her video game interface and smart television not only entertain her, they may also record her activities and conversations. Her computer webcam and items such as baby monitors also record information about her and her family. All of these technologies allow Hilda to be observed often in very intimate ways. The more devices and the more they are connected – with or without her knowledge – the more complex the networked system of data collection. Hilda might be aware that some of this technology collects and transmits extremely detailed and personal data about her to manufacturers and she might perhaps be comfortable about this, because she might believe that the company's collection of her data is secure and done in her interests, perhaps to improve services. Or perhaps she might not really have thought about it. However, what she may be unaware of and what she is unlikely to have really "agreed" to is the interception or transmission of that data to third parties who seek to monetize her data, hackers who seek to infiltrate her home, and whatever Big Brother wants her data. Regardless of her belief that her passwords are secure, many of these technologies are in fact inherently insecure and through this insecurity they expose her most private life to the world. Combining these technologies means the potential for almost constant surveillance and the generation of massive amounts of data – the ultimate in "Big Data" at

both nature (genetics) and nurture (environment) levels. The emergence of direct-to-consumer genetics, smart phones, wearable devices, smart meters, smart cities, and other (bio) technologies mean that private and public entities are amassing vast quantities of semi-structured, cross-referenced heterogeneous data about individuals and populations -- from information about their basic biology to insights about their actual and predicted behaviours. This White paper challenges you to think about this world of dynamic surveillance and whether living in a panopticon is something that is desirable for citizens? It aims to highlight some of the issues when data collected from this range of technologies are combined and encourage debate about not just appropriate legal regulation of these technologies, but the opportunity costs of pursuing their research and development as well as the right of citizens to not accept their deployment – to reject panoptic studies of humanity. Is it time to apply the Precautionary Principle to smart computing? In essence, what constitutes responsible technological innovation?

Smart Security at Airports – Smart for Whom?

Andreas Baur-Ahrens, a.baur-ahrens@uni-tuebingen.de, University of Tübingen
Marco Krüger, marco.krueger@izew.uni-tuebingen.de, University of Tübingen

‘Smart security’ has become an umbrella term which embraces several initiatives currently proposed by the aviation industry in order to enhance security procedures at airports. The idea of smarter security opposes the so-called traditional security framework of passenger security at airports. The latter stems from the 1970s and 1980s and uses a one-size-fits-all approach in order to detect dangerous items that might threaten flight safety and security. The industry claims that smart security provides better security, less intrusive security screening and better cost efficiency by employing tailored security procedures based on individual data-driven risk assessment of passengers and corresponding different levels of security screening. In our paper, we distinguish a set of meanings and reasonings behind smart security initiatives at airports from different perspectives. The contribution draws on several expert interviews. Inspired by assemblage theory, we identify several intertwining argumentations and materialities of aviation security that form the concepts and initiatives of smart security. We find that in the discourse security arguments are of less importance although often named first. In contrast, a better passenger experience and, above all, the aim to save costs by tailored and therefore also reduced security screening for presumably low-risk passengers are key to smart security initiatives. Moreover, human rights implications of smart technology, data-

driven risk assessment, decision making and sorting of citizens into risk groups are downplayed. Bearing in mind the severe consequences of computer-based sorting of humans into risk-groups and decision making affecting humans' mobility, we want to provide a thorough assessment of the driving forces of smart security in order to have a critical and ethically founded stance on these developments.

Education

Openness versus Privacy? Negotiating Value Conflicts for Open Source Inspired Privacy Education

Karen Louise Smith, karen.louise.smith@utoronto.ca, Brock University

Open source software is typically described as software where the source code is made available for others to examine, alter, and redistribute. Mozilla's Firefox web browser is one of the most globally recognized examples of open source software. Numerous privacy enhancing technologies, such as Tor, are also built as open source software. In 2014-2015, the Office of the Privacy Commissioner of Canada granted a Contributions Program award to Mozilla in Toronto, for a project to engage and educate the public in relation to the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA). The award enabled the formation of a project team involving scholars, practitioners, and 8 teen peer researchers who aimed to create an ecosystem of 10 prototype level open, privacy badges. In brief, open badges utilize an open technical standard to enable individuals to display their learning online. The project convened the peer researchers over 70 hours of project engagement, to co-design a badge system suitable to encourage young people to explore privacy issues in informal learning settings, such as libraries and community centers. This paper argues that value conflicts are present but negotiable, when utilizing participatory design methods to develop open source inspired curriculum relevant to privacy. Value conflict is an issue that is acknowledged to emerge in the design process. The visibility and transparency of open source software can sometimes be seen to conflict with privacy rights. Participatory design is a research tradition where the interrogation of democratic values, such as openness and privacy, is encouraged. This paper examines the discourses, such as design manifestos, relevant to value conflicts involving privacy in open source software projects as well as empirical examples of conflict from the participatory design workshops held with youth. Through the participatory design workshops, youth grappled with the

traces of their digital footprints and broader social issues related to the surveillance of education were surfaced.

From "zero tolerance" to "safe and accepting": Surveillance and equality implications of educational policy related to "cyberbullying"

Jane Bailey, jbailey@uottawa.ca, University of Ottawa

Schools are well-established spaces of surveillance through use of both technological devices (Taylor, 2014; Monahan, 2010) and basic classroom and school yard practices of interpersonal watching. Students' connectivity increasingly contributes to the seamless integration of various aspects of their lives by, among other things, giving connected students an unprecedented ability to surveil their peers (Steeves, 2014; Bailey, 2015). Technologized conflation of in-school and out-of-school spaces carries with it social interaction and connectivity, involving both positive and negative experiences (Bailey, Steeves, Burkell & Regan, 2013). On the negative side, digital communications technologies enable the seepage of "bullying" behaviours into spaces beyond the four corners of the school yard (Shariff, 2007; 2014). Thus, so-called "cyberbullying", which frequently involves identity based harassment (Bailey, 2013), has become a challenge for the education system. How the system responds could significantly impact the nature and level of surveillance to which all students are exposed. This paper will analyse various trajectories of Canadian education policy responses to "cyberbullying", both in terms of their implications for increasing surveillance, and for exposing certain equality-seeking groups to disproportionate surveillance. Part I will briefly introduce and analyse some of the policy issues that have arisen from cyberbullying, including jurisdictional concerns. Part II will focus on the "zero tolerance" approach, contextualizing it as part of a broader "law and order" agenda, with negative implications for equality-seeking groups (Skiba, 2014; Harvard, 2000; Bhattacharjee, 2003). Part III will analyse the transition in provinces such and Ontario and British Columbia to the "safe and accepting schools" model, tracing that model's relationship to concerns around the disproportionate targeting of LGBTQ students. Part IV will focus on curricular approaches in which addressing underlying individual and systemic factors, discrimination and misinformation are dealt with directly through curricular reform, commenting on trends in empathy training, encouraging involvement of bystanders and human rights training around issues of sexual identity and consent.

E-assessment or 'learningveillance'? The social impact of EdTech and the right to privacy for children

Iris Huis in 't Veld, iris@eticasconsulting.com, Eticas Research & Consulting

The times when teachers said "get your notebooks out" and did not refer to a computer are over. As society is becoming highly infused by technology, so is education. Governments and philanthropic organizations are investing high amounts of money in technologies for schools to create classrooms that are fit for the 21st century (Massy, 2016). When it comes to surveillance we easily relate it to Edward Snowden and governments collecting data, but actually few contemporary spaces are as thoroughly surveilled as the classroom (Rosen and Santesso, 2014). Monitoring students is not a new phenomenon since the same is done with attendance registers, timetables and examinations, but the rapid proliferation, the variety of technologies and number of devices installed enable schools to "identify, verify, categorise and track pupils in ways never before thought possible (Taylor, 2014, p.1)". In education a certain degree of surveillance is needed and even embraced, therefore student privacy should be looked at from a unique perspective. However, there is a lack of understanding of the meaning of privacy for children in schools. To what extent is surveillance in schools is morally justified and when is it an unacceptable infringement of privacy? I will discuss surveillance and privacy in relation to the school itself to see whether the effects of the surveillance fit the goals the institution has set out to achieve. This analysis will provide guidance for a socially sustainable future of EdTech design and policy.

Always Already Monitoring: School Surveillance of Young People's Social Media

Leslie Shade, leslie.shade@utoronto.ca, University of Toronto, Faculty of Information

Social media is one of the top activities and sites for young people's socialization in North America. This popularity and prevalence of use raises concerns both over young people's social privacy, because of reported increases in cyberbullying and sexting, and their informational privacy, due to the business model of commercial data collection by popular platforms. Schools and school districts, particularly in the U.S., are grappling with how to manage and monitor social media use by their students, both during and after-school, in order to prevent or lessen the perceived propagation of threats, violence, bullying and hate directed towards other students or entire schools. This has led some school districts to deploy third party applications and software to monitor, control, and track the postings of students, under the guise of securitization and responsibilization. Capitalizing on these moral panics, a new regime of parental and school monitoring tools that surveil the social media of

children and young people have been developed, taking off from the earlier marketing to parents of GPS mobile phone devices and subscription-based social networking sites that situated surveillance technologies as normalized and domesticated (Shade, 2011). In many ways these newer surveillant devices exemplify what Shoshana Zuboff refers to as “surveillance capitalism”: “a new form of informational capitalism [that] aims to predict and modify human behavior as a means to produce revenue and market control” (2015, p. 2015). This paper will provide an overview of these monitoring tools and companies (for instance, Geo-Listening, Varsity Monitor, Snap Trends, Digital Fly) and consider the policy and ethical issues of such intense data monitoring with respect to young people’s rights to privacy and their freedom of speech. --Leslie Regan Shade. (2011). Surveilling the Girl Via the Third and Networked Screen, pp. 261-275 in Mediated Girlhoods: New Explorations of Girls’ Media Cultures, ed. M. C. Kearney. NY: Peter Lang Publishing. --Shoshana Zuboff. (2015). Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. Journal of Information Technology 30, 75–89.

Rhizomatic educational technologies: Dataveillance and the digital school

Selena Nemorin, selena.nemorin@monash.edu, Monash University

The past decade has seen rapid growth in ‘new’ surveillance technologies in public schools. Traditional analog modes of school surveillance such as attendance registers, teacher monitoring, feedback and reporting, testing and examinations can now be performed online. Students and teachers find themselves under continuous watch, with (in)dividualized data and information captured and circulated inside *and* outside of school amongst a variety of (un)known actors. To date, surveillance in school has tended to be studied through a Foucauldian lens. Yet the increasing digitization of schooling has changed the nature and form of surveillance in terms of blurring boundaries of time/space, fixed/mobile, public/private. These shifts render the panoptic model incomplete as an analytic tool able to offer a comprehensive account of school surveillance in its diversifying forms. A complementary frame for understanding these emergent complexities is the ‘rhizome’ which has the capacity to illustrate the nature and reach of surveillance in digital schools. Informed by data generated from a three-year ethnographic study of three Australian high schools, this paper enquires into the surveillance practices at work in the digital school through a case study exploration of teachers’ use of Schoology, a learning management system (LMS). The online educational platform, this paper argues, supports pervasive rhizomatic modes of dataveillance - constituting both explicit and covert forms of surveillance that systematically monitor individuals

and/or groups through personal data networks in order to regulate or govern behaviours. The paper begins by approaching Schoology as a layered phenomenon: a technological artifact; how teachers were using the application; and wider contexts such as local and state policies. This is followed by a discussion of the artifact in relation to three principles of the rhizome: 'connection', 'heterogeneity', and 'multiplicity'. The paper ends with a consideration of the potential costs of Schoology as a form of rhizomatic surveillance, especially in light of continuing educational enthusiasms for learning analytics.

Public Administration

Categories that count: Methods and subjectivities in population statistics

Baki Cakici, b.cakici@gold.ac.uk, Goldsmiths, University of London

Different methods for generating population statistics enact different subjectivities, and changes in methods also bring about different subjectivities. Consequently, some groups are made more visible, while others disappear. Based on collaborative ethnographic research by a team of researchers at several European National Statistical Institutes, I analyse the different subjectivities enacted by different methods for counting the population. I focus on acts of categorisation where "problem subjects" cause methodological difficulties for statisticians. I introduce the Jedi census phenomenon from the 2001 and 2011 censuses in England and Wales to describe the challenges and surprises of category work by both the experts and the subjects, and I compare it to more recent experimental methods for categorising internal migration based on social media data. I argue that categories enact their subjects, and that acts of categorisation provide methodologically productive entry points for understanding subjectification. After a category is defined, it becomes possible for statisticians to identify those who fit that category, and the members of that category appear to have existed before the category itself. This is not to say that they do not exist as subjects prior to the act of categorisation, but that this particular subjectivity is performed in relation to the category, and the continued existence of the category sustains it. Moreover, the subjects perform the category differently, accepting it as it is, shaping it to suit their positions, or even rejecting it as an unwanted intrusion into their lives.

Negotiating welfare surveillance

Lars Bo Andersen, larsbo@dac.au.dk, Aarhus University

Peter Lauritsen, peter@dac.au.dk, Aarhus University

Peter Danholt, pdanholt@dac.au.dk, Aarhus University

Citizens in welfare societies are intimately related to, and supported by, various surveillance systems meant to support their education, healthcare, worklife, and so forth. Healthcare systems must know and surveil patient's health, school systems must know and surveil student's learning, tax authorities must know and surveil private income, and social services must know and surveil the upbringing of children from vulnerable families. In Denmark, a country with a highly developed welfare system, each development of the welfare state has traditionally been accompanied by public debate and concerns over the privacy of citizens. The premise for these concerns is typically that the more efficient the welfare system the less privacy for citizens, that welfare and privacy constitutes opposing poles in a zero-sum negotiation. In this paper we discuss the relation between welfare services and individual privacy in relation to a specific case from the social services where social workers are working to strengthen their relations with children placed in foster care or at institutions. We describe how children and social workers continuously negotiate a surveillant welfare relation allowing social workers to know the children well enough to care for their upbringing while enabling children to protect those parts of their life which they do not trust the social workers to know. The paper develops the argument that surveillant welfare relations are fragile, constantly negotiated and provides both social workers and children with oligoptic insights into each other's lives rather than panoptic invasion of children's privacy. In fact, both children and social workers struggle quite hard to establish relations relevant and formative for them to do their job and live their life.

Communications surveillance in the UK: politics, governance and regulation

Wil Chivers, chiverswg1@cf.ac.uk, Cardiff University

This paper reports on empirical research examining the regulation and governance of surveillance. Employing a social constructionist perspective, the paper emphasises how legal frameworks that seek to re-organise and regulate the infrastructure of digital/communications surveillance in the UK also generate effects of resistance. Consequently, the research identifies the various claims-makers who advocate or oppose changes to this infrastructure and examines the nature of their claims.

The paper draws on empirical data from analysis of the publication and response to two pieces of UK legislation: the Communications Data Bill (2012) and the Investigatory Powers Bill (2015). It is suggested that, as well as mobilising public attitudes against such proposed changes to the digital surveillance apparatus, these frameworks illuminate the negotiated character of the governance of surveillance. Specifically, developing the concept of 'mediated surveillance' (Bright and Agustina 2013), the role of private sector communications service providers in this process is highlighted. The paper concludes that while significant changes in the landscape of global surveillance 2012 to 2015 have impacted on the way in which the law is designed to regulate so as to accommodate the need for both privacy and security, there may be more negotiation yet to be done.

Does counting change what's counted? Performance management and the resurgence of positivism in Norwegian sociology

Ann Rudinow Saetnan, annrs@svt.ntnu.no, NTNU

Gunhild Tøndel, gunhild.tondel@ntnu.no, NTNU

Bente Rasmussen, bente.rasmussen@svt.ntnu.no NTNU

Watching, measuring, counting is, according to some, a non-invasive form of interaction. Supposedly, what we see/measure/count is simply what is, regardless of our gaze. This paper examines whether the new surveillant practices of performance management are having effects not only on the productivity of academic work, but also on its content. To use Karen Barad's terms, is the measuring device a part of, and thereby affecting, the phenomena being measured? Taking a broader view, what does this say about surveillance in general? Should we be re-exploring the intra-actions of surveillance and society, looking for new forms of optic effects?

Policing

Covert policing and the infiltration of protest groups in Britain

Raphael Schlembach, r.schlembach@brighton.ac.uk, University of Brighton

This paper draws on ethnographic research and interviews with environmental campaigners in the United Kingdom who have been subjected to extensive surveillance and infiltration by undercover police officers. The activists are at the centre of the controversy surrounding the deployment of covert

human intelligence sources to infiltrate left-wing protest groups across Europe. In 2010, these campaigners were able to expose the identity of several key undercover operatives, which, after extensive media reporting and official investigations, has triggered a public inquiry led by Lord Justice Pitchford. The research participants have 'core participant' status in the Pitchford inquiry. Though the inquiry's remit is restricted to England and Wales only, there are implications for our understanding of the international deployment of British undercover officers. The picture of undercover policing that has emerged so far gives ground for a re-assessment of the character and legitimacy accorded to the 'British model of protest policing'. To contribute to more theoretical debate, I further argue that the covert policing of protest offers a lens through which to re-evaluate the relationship of criminological research to political dissent.

Struggles For Visibility: On the Exhibition of Police Violence in a White Democracy

Ben Brucato, ben@benbrucato.com, Amherst College

Police developed in modern democracies as the primary institution that would produce the social order through articulating state violence against those identified as threats to it while within their borders (Neocleous, 2000). Also crucial during this time—and therefore to this development—was the elimination of the spectacle of state violence as a key means of social control (Foucault, 1979). Violence has always been fundamental to policing (Bittner, 1970; Klockars, 1985). Nonetheless, its violence was historically removed from broad public view (Skolnick & Fyfe, 1993). Police have always strategically modulated their visibility to maximize their power. Today, however, partly as a consequence of surveillance and sousveillance technologies and the use of the documents they produce, policing has encountered new visibility, a visibility not as often under the control of the institution (Goldsmith 2010). Many academics, politicians, journalists, and activists anticipate that since police no longer have as much control over when, where, and how they are visible to publics, the power of the institution and its agents to avoid accountability for wrong-doing is in jeopardy (Anthony & Thomas, 2010; Fan, 2012; Jeffries, 2011; Koskela 2009; Robinson, 2012; Stuart, 2011; Toch 2012; Wilson & Serisier, 2010). Concomitantly, they expect that because civilians are increasingly capable of producing the mediated visibility of police through sousveillance, these civilians are thereby empowered (Diamond & Platner, 2011; Yesil, 2011). As a consequence of this seeming consensus, advocates for those victimized by police—or for "police accountability"—likewise have a nearly uniform response that increasing the video documentation of policing is of

certain advantage (Brucato, 2015; Brucato, forthcoming). John B. Thompson (2005) has established that political controversies are products of and are negotiated through "struggles for visibility." Taking this condition as a point of departure, this paper explores this new visibility of police violence in the United States as a white democracy. Olson (2004) describes "white democracy" as a condition where there is "democracy for whites, tyranny for everyone else" (p. 71). The description of popular sousveillance as enabling "transparency" fails to acknowledge the fragmentation of the polity—and therefore audiences—along what W.E.B. Du Bois called "the color line" (Brucato, 2015). The presumption that the visibility of the racist qualities of criminal justice institutions will spur popular outrage homogenizes audiences in ways that are analytically and empirically unsustainable (Waddington, Williams, Wright, & Newburn, 2015; Cheliotis, 2010). Furthermore, this approach ascribes to viewers commitments to cross-racial identification and solidarity that are rarely demonstrated (Brucato, 2015; Thompson & Lee, 2004; Weitzer, 2002). Instead, the visible itself is racialized (Butler, 1993). Since most of those victimized by police are not white, their advocates must engage struggles for visibility as contentions over the very nature of—and, indeed, the automatic recourse to—the visible.

Policing & Communities

Tackling new security challenges through community policing and the use of information and communication technologies (ICTs)

José María Zavala Pérez, josemaria@eticasconsulting.com, Eticas Research & Consulting

In the wake of budget constraints and shifting security concerns, a combination of Community Policing (CP) principles and technological applications provides an enhanced concept of security through a more dynamic, direct and close relationship between law enforcement agents (LEAs) and the citizenry. A thorough consideration of the societal and ethical challenges of community policing has proven to be an important step for developing best practices and for integrating information and communication technologies (ICTs) into these practices. Such considerations ensure that new initiatives support police departments and officers in their daily work, help integrate citizens and nourish positive community-police relationships while minimizing negative externalities such as bias, discrimination or a negative impact on social cohesion. In order to appraise the societal aspects of technology-mediated community policing it is important to focus on their broad scope of applications, whereas the societal impact of technological developments can be explored according to four sub-

dimensions: desirability (the actual need of a certain technology), acceptability (the extent to which a technological innovation will be welcomed by a community), ethics (the shared values and moral standards embedded in a society) and data management (the consequences a system may have regarding privacy and data protection). Furthermore, a set of four legal dimensions was assessed in order to cover the elements that need to be taken into account for the implementation of the project: democratic rights and civil liberties; LEAs and security; privacy issues; ICTs, media and communication.

Police as Law Makers: Tracing the Making of Canadian Anti-Masking Legislation

Debra Mackinnon, 14dmm3@queensu.ca, Queen's University

Days after the June 2011 Stanley Cup riots, Canadian law enforcers and lawmakers, facing criticism for the poor control of protests and riots turned to other jurisdictions for policies and best practices. Introduced to parliament as a private members bill, The Preventing Persons From Concealing Their Identity During Riots and Unlawful Assemblies Act became law on June 19th, 2013. Also referred to as Bill C-309, this anti-masking legislation makes the wearing of a mask during a riot an indictable offense. By expanding the paramilitary policeman's "tool kit" – already outfitted with long-range acoustic devices, water cannons, anti-bandit glass, rubber bullets, and full tactical gear – this anti-masking legislation prepares bodies as sites for exposure and capture; thereby optimizing the surveillance-ready-subject. Masks become a way of constructing and then identifying the illegal and the unlawful. Drawing on Access to Information and Freedom of Information releases from municipal, provincial and federal governments between 2008 and 2013 this paper explores the role of police as researchers and law makers. The early work of prominent British Columbia police chiefs and various officers in the making of Bill C-309 problematizes the role of police as solely law enforcers. Law and its implementation, rather than limited to the executive and legislative branches, is ultimately dependent on those who enforce it (Lipsky, 1970). However, this classic and conservative conception of jurisdiction fails to acknowledge the various scales and levels of governance that police are operating on and within.

Good Cops, Bad Citizens and the Quest for Security: Lawyers as agents of the state in anti-money laundering

Karin Svedberg Helgesson, karin.svedberghelgesson@hhs.se, Stockholm School of Economics

Ulrika Mörth, ulrika.morth@statsvet.su.se, Stockholm University

This paper analyses the relationship and interplay between (external) demands for more surveillance and risk management, and (local) ways of handling, adapting to, and/or resisting these demands. We are particularly interested in how local actors deal with issues of accountability, responsibility, and blame in relation to surveillance and risk management: To whom are they (agreeing to be) accountable? What are the boundaries of their responsibilities? And how do they avoid – or take – the blame? The paper is based on an interview study with law professionals in the UK and France, and focuses on how these actors handle increasing demands to engage in surveillance of clients as set out in transnational risk based regulation on anti-money laundering/counter terrorism financing (AML). We analyse to what extent lawyers take on and engage in surveillance of clients, with a view to how these obligations are handled in their everyday practice. We find that regulatory demands to engage in surveillance of clients and manage risks of money laundering have had an impact in both empirical settings. The risk of 'money laundering' is now an object of risk that lawyers recognize and are able to deal with. We further find that UK lawyers primarily reported what they deemed to be 'nonsense'. But it was not any nonsense, it was the nonsense that law enforcement and competent authorities had asked for. By putting time and effort into nonsense, UK lawyers strove to avoid blame, all the while keeping business interest close to heart. Among French lawyers, the responsibility for AML, and the boundary between what was laid out in the regulation and actual crime prevention, was less clear. In principle the responsibility for AML surveillance and reporting lay with the individual lawyer. In practice, reports were scarce, and lawyers hesitant or out right resistant. French lawyers, and their professional bodies, did not appear as worried about protecting themselves from blame in relation to money laundering risks as their British counterparts. Rather, they were preoccupied with two other risks. The first was the risk of breaking client privilege, and the second the risk of being considered an informer to the state. Taken together, these two risks were considered more severe than the risk of AML, and, consequently, avoiding blame in relation to these other risks was higher on the agenda. In conclusion, where UK lawyers strove to achieve a balance between the demands for surveillance of the (AML) regulator, the client and the profession, French lawyers privileged the client and the profession.

Good Cops, Bad Citizens and the Quest for Security: Lawyers as agents of the state in anti-money laundering

David Murakami Wood, dmw@queensu.ca, Surveillance Studies Centre, Queen's University

During the last fifteen years, the global city of Tokyo has seen the diffusion of public open-street video surveillance and a prolonged period of neoliberal spatial restructuring. A qualitatative longitudinal study comprising several research visits to one small community association in central Tokyo over this period provided the opportunity to examine changes in the way that members have changed their ideas about surveillance and public safety. In particular, the transformations in conceptualisations of trust (social assurance) and how ideas of safety and danger attach to particular places were examined over this time, through site visits and conversations. As a microsociological study, broader conclusions must be drawn with care, however the findings were that the diffusion of video surveillance had three stages: the introduction at first provokes concern and fear and a loss of broad social assurance; 2. surveillance is gradually normalised, becomes something that is participatory, and trust returns in a reconfigured and more specific way; but 3. a further stage occurs in which both disillusionment and the search for more holistic solutions to social problem begins to emerge.

Digital citizenship and Surveillance Society: State-Media-Citizen Relations After the Snowden Leaks

Chair: Arne Hintz, hintza@cardiff.ac.uk, Cardiff University

This panel will present findings from the 18-month ESRC-funded research project "Digital Citizenship and Surveillance Society"(October 2014 – March 2016) which explores the nature, opportunities and challenges of digital citizenship in light of the governmental surveillance measures revealed by whistle-blower Edward Snowden. The revelations have prompted significant debates on the nature of civil rights in a context of security; the extent of state interference in civil life; the accountability of government agencies and corporate intermediaries; the uses of technical infrastructures; and the role, responsibilities and limitations of journalists reporting on state activities. This project analyses the implications of the Snowden leaks in four areas that constitute key components of digital citizenship: 1. Civil society, advocacy and activism; 2. Media coverage and press freedoms; 3. Technological infrastructures; and 4. Policy, law and regulation. The project's investigators will present the research results and will discuss what they mean for notions of digital citizenship. This panel will serve as the first international venue for the project's different thematic streams to come together at the end of the project period, present the final research results, and discuss them with international surveillance scholars.

Civil Society Responses to Surveillance

Lina Dencik, dencikl@cardiff.ac.uk, Cardiff University

Drawing on research carried out for the project's civil society workstream, this paper will present key findings on the implications of the Snowden leaks in two different areas concerning civil society: a) public knowledge and attitudes towards issues relating to surveillance; and b) political activism. Based on focus groups with different demographic groups of the British public as well as in-depth interviews with a number of prominent activist groups in the UK, this paper will discuss public understandings of surveillance, concerns regarding personal data, and changes in online behaviour, or lack thereof, since the Snowden leaks. Looking at attitudes and practices amongst the general public as well as political activists in particular, it will explore the level of acceptance of surveillance, areas of concerns, manifestations of online self-censorship, and a possible 'chilling effect' on dissent and resistance.

Media Reporting of Snowden and Surveillance

Karin Wahl-Jorgensen, Wahl-JorgensenK@cardiff.ac.uk, Cardiff University

As part of the project's media workstream, this paper will outline some of the key narratives and debates that have marked the coverage of the Snowden leaks in the British press by focusing on a number of key events since the revelations first entered public debate. These include the initial exposure of the PRISM and Tempora programmes, the monitoring of foreign embassies and spying on heads of state, the detention of journalist Glenn Greenwald's partner, David Miranda, and the controversy around the report into the death of Fusiller Lee Rigby, which generated debates around the further monitoring of online communication. This paper examines the coverage of these events in the British national press using content and framing analysis to demonstrate the portrayal of Snowden himself, the opinions expressed by the newspapers in relation to mass surveillance, and the major issues and debates which have arisen from these revelations. This will be supported with findings from in-depth interviews with journalists regarding the implications of the Snowden leaks for journalism and press freedom.

Technological Standards and Infrastructures

Grace Eden, grace.eden@hevs.ch**,** University of Applied Sciences of Western Switzerland

The Snowden leaks reveal a complex network of state surveillance programmes that collect, store and analyse massive amounts of digital communications on a global scale. Indiscriminate access to personal information has serious implications for, particularly, high-risk users of digital communication tools such as journalists, activists, whistle-blowers and others and has led to a reassessment of the ways in which they communicate digitally. Drawing from interviews with members of relevant international institutions, this paper will discuss the role that standards organisations play in the undermining of citizen privacy by agreeing to technically weak implementations of protocols that maintain the Internet infrastructure. For example, this is done by organisations such as NIST and IETF agreeing to the design of 'backdoors' within standards. We will also discuss the increased need for citizens to use privacy-enhancing tools (PET) in their day-to-day digital lives and contrast this with the lack of training in their use which leads ordinary citizens to lack confidence in choosing the right technologies or the knowledge of how to use them appropriately.

The Regulatory Context of Surveillance and Policy Reform

Ian Brown, ian.brown@oii.ox.ac.uk, Oxford University

The regulatory environment of surveillance is obscure, as review efforts such as the Anderson commission in the UK have observed. Policy reform after Snowden has been inconsistent, ranging from the extension of surveillance capabilities (such as the DRIPA Act in the UK) to cautious restrictions to surveillance (such as the USA Freedom Act) to significant objections (e.g., the decision on data sharing by the European Court of Justice). We will discuss this policy landscape with the help of an online database and hyperlinked encyclopaedia that was built as part of this project, and that allows users to navigate through pages detailing various surveillance powers, relevant laws and guidelines, and the different state actors involved. We will also share notable findings and recommendations harvested from a series of interviews with high-level representatives of government, industry and advocacy involved in the ongoing policy debate.

Digital Citizenship in the Age of Mass Surveillance

Arne Hintz, hintza@cardiff.ac.uk, Cardiff University

The aftermath of the Snowden revelations has seen the intersection of two different narratives. On the one side, the empowering nature of citizen journalism, social media activism, participatory online communication and, not least, bottom-up ‘sousveillance’ of elites and institutions has suggested a shift towards enhanced agency by citizens and a democratising trend in state-citizen relations. On the other side, the pervasive monitoring and analysis of people’s digital communication, movements, activities and preferences by both states and the private sector have led to unprecedented capabilities to oversee and, by extension, control the citizenry. In parallel to these opposing trends, the role of (and perceived ‘balance’ between) state security and civil rights is negotiated in public debate. This paper will unpack these developments and explore their meaning for the future of digital citizenship. Based on findings from the research project ‘Digital Citizenship and Surveillance Society’, as well as research on activism, censorship and commercialisation in online environments, I will argue that we are witnessing the emergence of a supervised form of citizenship in which individual capabilities to engage with one’s environment are expanding but are, at the same time, tightly monitored, policed and controlled.

Surveillance and the Construction of Identity and Evidence in Criminal Justice Systems

Mehera San Roque, m.sanroque@unsw.edu.au, Faculty of Law, University of New South Wales
Benjamin Goold, goold@allard.ubc.ca, Allard School of Law, University of British Columbia

We are proposing a panel that would address diverse ways in which surveillance technologies are utilised within the criminal justice system, broadly conceived. The rapid proliferation of CCTV and other surveillance mechanisms has given rise to an ever expanding gallery of images and other surveillance artefacts, including biometric data, that can be invoked in the attempt to identify and prosecute those engaged in (potential) criminal or anti-social activities. Surveillance Studies has paid substantial critical attention to what are often characterised as the exceptional privacy and human rights implications of the expansion of (preventative) surveillance, but in doing so has tended to rely on a relatively narrow conception of the regulatory potential, force and direction of law. This panel seeks to develop a more nuanced understanding of law and legal regulation–considering the role of surveillance technologies in day-to-day policing, as well as the admission and reliance on surveillance artefacts in the quotidian criminal trial. Participants will explore attempts within criminal justice systems to manage and exploit the expanding surveillance archive, situating their analysis within the context of both traditional and evolving modes of policing and other law enforcement activities, and paying particular attention to the role of surveillance in the fixing of social, professional and criminal identity. Topics include the emergence of 'super-recognisers' as experts in identification within police forces and for courts; police adoption of novel visual monitoring technologies; relationships between surveillance, mass disturbances and moral panics; and the ways in which undercover police both perceive and manage their relationship to legal regulation.

Games of Power: Strategies of Dominance, Submission and Resistance in Criminal Identification Practices

Diana Miranda, dianam@ics.uminho.pt, University of Minho

This presentation explores the meanings attributed to criminal identification practices by Polícia Judiciária's inspectors (responsible for these proceedings during the criminal investigation) and by

convicted offenders (the main target of these practices). Through a qualitative theoretical-methodological perspective and based on a set of semi-structured interviews and informal conversations, we analyse the perceptions of these actors regarding the use of criminal identification technologies. In particular, we will focus on fingerprint and DNA technology, since these are considered the most useful and efficient identification methods in criminal investigation. We explore the collecting procedures of fingerprints and biological samples and consider the implications that these procedures create. There are relations of power that should be seen as a strategic game where the dynamics of domination, submission and resistance endure. Despite the different reactions from the individuals subjected to these practices, they can be aggregated in situations of embarrassment, consensus and rejection according with the dynamics of the game.

Counter Law or Club Law? Surveillance, Membership and the New Public Order

Ian Warren, ian.warren@deakin.edu.au, Deakin University

Contemporary surveillance and urban securitisation practices are often underpinned by law against law, or counter law. The counter law thesis questions the removal of due process requirements, largely focusing on the increasing hybridisation of criminal law. For example, extensive work by British criminologists, including Zedner and Crawford, pinpoints the 'interpenetration' of contractual and administrative law principles in the management of antisocial behaviour, which simultaneously aims to improve efficiency and effectiveness in the administration of justice and crime prevention. Counter law skews the balance between the rights of the suspect and community protection, by removing formal legal requirements to be informed of the allegation, to contest prosecution evidence or be exposed to proportionate and determinate punishments. Such measures are counter to foundational criminal law precepts. One pertinent and emerging site of interpenetration into the criminal sphere involves the complex area of 'club law'. Club law is a branch of private administrative law that applies to closed or exclusive communities, including professional associations, sports clubs, or voluntary associations. A central element of club law is the ability to regulate inclusion or exclusion through the development and administration of membership criteria, which promotes internal club surveillance through self-regulation. This paper offers two examples from Australia and Canada that demonstrate the linkages, complexities and counterintuitive nature of club law in managing urban public order. Each case highlights the centrality of surveillance in producing a form of desired social membership in privately managed public areas within a hybridised club law framework. Both cases centre on the

power to ban, yet produce starkly opposing results through equivalent legal principles that were originally developed to promote highly idiosyncratic 'club goods'. Contra the counter law thesis, the paper suggests 'club law' and its emphasis on surveillance through membership represents the new 'normal' in contemporary urban governance.

Theory

Ludic surveillance – the strong profit, the weak lose?

Liisa A. Mäkinen, liisa.a.makinen@helsinki.fi, University of Helsinki
Hille Koskela, hille.koskela@utu.fi, University of Turku

Surveillance has become inconspicuous. While surveillance is able to expose anyone, people have become increasingly fascinated by creative ways of using surveillance for purposes reaching beyond social control. People use surveillance in ludic settings. Many scholars have noted the analytic importance of playfulness, challenging the boundaries between surveillance and entertainment. Surveillance has many playful functions not yet been addressed in their full extent There is no single context of surveillance and play, but multiple players with shifting motives. In this presentation we focus on ludic surveillance practices. Catching of someone in the act is one of the most common motives for the monitoring of places and people. So is revealing or witnessing something. There are clear conceptual links to plays such as cat-and-mouse and hide-and-seek. Further, surveillance increasingly takes place in labyrinth-like settings in which people navigate through multiple forms of control. These surveillance labyrinths are constantly changing and challenged. Intense surveillance may also lead to increasing mistrust. We argue that faking, tricking and camouflaging have become persistent elements of contemporary culture: counter-surveillance practices resemble circus tricks. Moreover, it must be acknowledged that some tricks are vicious: while someone wins, someone else is losing. In real life these oppositions are never clear as the roles and the motives of surveillance players are constantly changing. In this presentation we aim to discuss the complex connections between enjoyment and control. Examining the ludic elements of surveillance facilitates a broader understanding of how these practices move beyond power and discipline. We discuss both the positive effects of ludic surveillance and the alienating outcomes in which 'real people with their real lives' disappear and the playful subjects lose full understanding of the consequences of their playful practices.

Surveillance in a Hall of Mirrors: Autonomous, Amoral, Autopoietic

John MacWillie, jmacwillie@cal.berkeley.edu, California State University - East Bay

Surveillance has passed from an age of social engineering -- the observation and manipulation of social relations accomplished through the medium of human beings -- into one in which images are infinitely regressing into points of diminishing resolution such that the social subject is indistinguishable from the flicker of digital protocols -- LTE, MPEG, RFID, TCP/IP, AES -- floating through the ether. This transformation is the result of the entanglement of surveillance with the trajectory of technology, so much so that it begs the question of whether the future of surveillance is more technological, than social. In consideration of this shift, we need to reconsider the ontological status of surveillance and the significance of its convergence with technology. For example, Foucault famously proposes that the origins of modern surveillance are founded out of the institutional interests of discipline and enclosure, represented emblematically by Bentham's Panopticon. Deleuze proposes that the interiority of these same institutions have deteriorated to the point that discipline is ineffective, and has been succeeded by "societies of control" which "modulate" and accommodate differences. However, in systems of both discipline and control, the human being is the object of order. There is, however, an emerging alternative wherein the object of order is not a human being, but of order itself (meta-surveillance), such that human beings are simply incidental effects of the process of technical ordering. Shut-out of this practice altogether, human beings are left with few options apart from a paranoia that normalizes the act of suspicion. This is the technological surveillance envisioned by Philip Dick. Working from a set of new media and cognitive theorists, this paper proposes to explore the characteristics of next-generation surveillance that is driven by the exigent requirements of technology. Among the most important of these are technologies that increase agent autonomy, disengage techno-cognitive processes from human prejudices and ethics, and are self-sustaining and autopoietic. Each of these factors will be illustrated by current pilot projects or laboratory initiatives in military and law enforcement applications.

What is surveillance? How defining surveillance can support the growth of surveillance studies

Francesca Menichelli, francesca.menichelli@crim.ox.ac.uk, Centre for Criminology - University of Oxford

This paper tries to provide an answer to a deceptively simple question: what is surveillance? The central idea that it proposes is that surveillance needs to be understood as a mode of ordering, a strategy that is deployed – either in itself or, more commonly, in support of other governmental strategies – in order to provide a solution to a perceived problem of governing. Under this light, it follows that surveillance is not specific to any given context, scale or society. In turn, this means that, order being in itself a recursive process of construction and reconstruction, surveillance will structure recursively any context or society in which it is adopted. Concurrently, however, different contexts, scalar arrangements and social configurations will also impact on the specific and contingent forms that surveillance as a mode of ordering can take, on the discursive regimes that are used to justify its deployment and on the goals it is called to contribute to achieving. I believe this approach is crucially important in three distinct, but related, ways. First, in widening the definition of its titular object it broadens the scope and depth of surveillance studies towards the acknowledgement of the surveillant features of developments and innovations that are not commonly considered under this light, and of the implications these raise in terms of privacy, transparency, accountability and social justice. Second, the idea of surveillance as a mode of ordering opens the door to a consideration of the networks and assemblages that emerge dynamically around it, and whose exploration is instrumental in analysing concrete configurations of governance, and how power and resources flow in them. Lastly, this makes it possible to do away with some of the unspoken assumptions that have given the field of surveillance studies its strong Anglo-centric and deterministic flavour. This is all much to the benefit of the continued development and growth of surveillance studies as a field of inquiry in its own right.

Art

Panoptic Art: surveillance under the perspective of the artists

Renata Barboza Carvalho, desligada@gmail.com, Universidade Presbiteriana Mackenzie
Wilton Azevedo, wiazeved@terra.com.br, Universidade Presbiteriana Mackenzie

Surveillance has became omnipresent in society. The hesitant behavior face to a surveillance camera is in the context of panoptic logic of the society control. Using cell phones, bank cards, surfing the internet or walking down the street, everybody has been watched. The line between the surveyor and the object of inspection is more tenuous as never before. All these issues concerning the practices and impact of surveillance have been investigated not only by sociologists or political theorists. Since decades, artists have been aware of surveillance issues and the panoptic art has take the role of identifying and bringing attention to it. The highlight is given to a particular work produced in 1983 by the German-based artist Michael Klier, Der Rieser, (The Giant) a visual symphony generated by video-surveillance cameras. This paper is drawn from a developing master's thesis research associated to the LHUDI – Digital Humanities Lab of the Mackenzie Presbyterian University, in São Paulo, Brazil. This publication was supported by Mackenzie Research Funding. (Publicado com apoio do Fundo Mackenzie de Pesquisa.)

Regulation by Design for Ambient Domestic Computing: Lessons from Human Computer Interaction

Lachlan Urquhart, lachlan.urquhart@gmail.com, University of Nottingham

This paper will look at the role of design in addressing regulatory challenges posed by ambient technologies embedded in our domestic environment. Many terms capture the essence of these technologies from internet of things and ubiquitous computing to ambient intelligence and home automation. Broadly we define these as technologies physically embedded around us that sense and process human data to provide contextually appropriate services. These systems have varying levels of visibility (physically and psychologically) and autonomy (from minimal to semi autonomous behaviour). They may prompt a direct interaction (eg through an interface or smartphone app) or/and try to understand our human needs by sensing our presence or movements (eg smart thermostats managing our home heating based on movement). The relationship between the human and ambient computer is one of daily interaction where technology often mediates routines and human

experiences in the home. The goal of many of these technologies is to become assimilated into daily life to the extent they become 'unremarkable'. There is often a complex ecosystem of actors involved in the provision of both devices and services, from the manufacturers developing and managing the systems, to the third party advertisers seeking access to the data. Increasingly we see policy and law moving towards involving non state actors in the practice of regulation. A key example is regulators looking to designers to enable regulation by design. From nudges to privacy by design we see a recognition of the power of design as a mechanism to address hard regulatory problems and the importance of designers as mediators. We recognise that the system designers of these new ambient technologies have a responsibility to their users and they act in some capacity as regulators through their ability to define how the human uses and engages with the technology. Importantly, the technology is not neutral, it is a product of active choices and decisions of system designers (from system architects and programmers to interface and user experience designers). We are particularly interested in human agency concerns, which are themselves broad. Narrowing down the problem space is problematic but user control over personal data, (dis)trust in the infrastructure and the importance of decision making and choice when interacting with these systems are particular interests. We consider the range of tools available to system designers within the field of 'human computer interaction' to address regulatory concerns. When designing new ambient technologies, HCI practitioners use methods to build situated knowledge of the practices in the social settings that technologies will be built for, from workplaces to homes and public spaces, often by speaking to and observing users of these systems. They do this to make sure the systems, experiences and interactions fit the context of use. These same design tools and knowledge could be repurposed to understand regulatory issues faced by users in context. Accordingly, we reflect on approaches from the HCI that help system designers engage with their regulatory role, eg value sensitive design or the Scandinavian school of participatory design.

Let's make and play PSS – Towards community involvement and participation

David Behar, davidbe@technion.ac.il, Technion

Despite of the increased interest and research in surveillance issues, for example the intensification and growing complexity of the public space surveillance phenomena, re-thinking and suggesting alternative approaches for public space surveillance have benefited from little academic attention. This paper addresses Public Space Surveillance (PSS) as an object of community based

investigation, involvement and participation. Coming from Art and Design action perspective, the writer, whose studio practice is public space situated, elaborates about the need to engage PSS with a bottom-up approach. The paper mentions the reasons why to challenge current surveillance methodologies (imbalance of power, inflexibility to community needs, loss of residents' confidence etc.), and questions whether neighbourhood residents do need to be dependent on external powers for their own security issues and needs. The-Right-To-The-City framework, as relating to ideas of Lefevre, Harry and Purcell is brought forward as a conceptual support for community involvement in public space security issues. Furthermore, the author is stressing the need to rethink and to reformulate the common rights for security, in difference to the public rights for security, in order to lay the groundwork for action-based change. The paper suggests that acting with the involvement of communities can be taken under the play and game conceptual umbrella, as a way to achieve beneficial community outcomes. This approach has the potential to encourage the subversive qualities of game phenomena to build up a critical reflection on everyday experiences and values as well as to cultivate ethical generosity. The author will also address how such alternative methodologies can function in the urban patch-plan of everyday neighbourhoods and suggest strategies for municipal co-governing.

Seeing through the 3rdi: Surveillant art and material visions of resistance

Laurel Ahnert, lahnert1@gsu.edu, Georgia State University

Jason Derby, jderby1@gsu.edu, Georgia State University

Recently, the comedian John Oliver interviewed Edward Snowden about the NSA surveillance leaks. In the interview, Oliver humorously, yet poignantly, demonstrated the general American cultural perception of the surveillance apparatus as something largely abstract, distant and unrelated to their daily lives. This brief example demonstrates a larger issue, namely that the political conversations regarding surveillance tend to assume a level of technological literacy and mobilize political or emotional investments which do not necessarily resonate with the public. Moreover, the perceived "immateriality" of electronic technology and the invisibility of the surveillance industrial complex render abstract these very real, material relations. Yet in this paper we suggest that, while the surveillance industrial complex strives to render its infrastructure invisible and immaterial, art can render visible the material and embodied nature of surveillance, and its consequences, on a wholly different register. Specifically, this paper will look at recent works of art that engage directly with and attempt to subvert the asymmetrical operations of surveillance. In 2010 Wafaa Bilal surgically grafted

a digital camera to the back of his head. Programmed to capture images at certain intervals, the camera cataloged and archived the images via the web. Bilal, an Iraqi American, designed the 3rdi (pronounced "third eye") project to reflect the unique realities of living as a subject of the U.S. surveillance machine. The 3rdi project rematerializes the seemingly immaterial and invisible processes of surveillance, demonstrating the violence of these operations of power in terms more affectively present than conventional technological and political discourses. More importantly, Bilal's work points to a form of aesthetic that resists the standard organizations of power within surveillance relations. Working through Jacques Rancière's supposition that art enacts a "redistribution of the sensible" we illustrate how the aesthetics of 3rdi intervenes in the field of politics by shaping perceptions of identity, belonging (and exclusion), experienced by surveilled subjects. Next we explore how this visual and embodied form of intervention provides resistance politics with an aesthetic vocabulary for criticizing the modern surveillance industrial complex.

Art and Film

'The Brave New World of Datamacy: Blurring Data and Intimacy in Spike Jonze's Her'

Peter Marks, peter.marks@sydney.edu.au, University of Sydney

This paper explores the ways in which Spike Jonze's 2013 Academy Award-winning film Her depicts and dissects potential trends in interpersonal relationships, ones that have intriguing and perplexing surveillance implications. If many of our most fundamental and consequential actions in a surveillance society are disembodied, and carried out via various forms of social media, it remains true that the ideal (or idealised) interpersonal relation is still figured in terms of face-to-face interaction. Her complicates this ideal in a very contemporary way, by projecting a relationship between the sensitive, shy Theodore Twombly and 'Samantha', an artificially intelligent operating system that utilises big data to fashion an attractive virtual 'identity', one with whom Theodore falls in love. The film incorporates and updates elements of the romantic comedy with a long narrative of utopian texts that deals with the 'problem' of intimacy. Significantly, Her creatively considers the ways in which the contemporary collection and deployment of data reconfigures individual identity, and with it the prospects of authentic interpersonal associations. We are entering what the paper labels

the brave new world of ‘datamacy’. Situating the film in an essentially eutopian near-future Los Angeles, writer-director Spike Jonze paints LA as a place of disconnected individuals drowning in surface ease and contentment, an artificial world underpinned by various forms of accepted monitoring, control, and privacy invasion. The paper aims to show and critically examine how Her shines a sharp an illuminating light on the modern intersection of surveillance and intimate relationships.

Drones over the Frontier: The Panopticon Border in Recent US-Mexico Border Films

Fareed Ben-Youssef, fben@berkeley.edu, University of California, Berkeley (Film and Media)

When framing the impact of policy related to the Drug War and War on Terror upon the US-Mexico border, political scientist Tony Payan concludes that “The Panopticon Border” has been created. Employing a framework that combines theorizations of the post-9/11 border with legal scholarship, my paper reviews a number of recent border films to articulate the myriad ways this panopticon has been visualized and critiqued. These films include Tommy Lee Jones’ nightmarish Western allegory "The Three Burials of Melquiades Estrada" (2005). Using metaphoric imagery that recalls a prison, Jones expresses the psychic plight of the illegal Mexican migrant who perceives visibility as a trap. In viral videos for Ridley Scott and Cormac McCarthy's parodic "The Counselor" (2013), the filmmakers suggest the omnipresence of police surveillance upon its border actors, figuring this sight as a kind of phantom. Denis Villeneuve’s border noir "Sicario" (2015) offers an ever-shifting view of the border, moving from the eye of American drones to Mexican families living near border walls. The film presents a magisterial final set piece that cycles between surveillance footage from the FBI’s night vision, the army’s infrared, and the CIA's drone view. The disorienting sequence creates a visceral appreciation of a state that reduces humans on the border to little more than specks and blurs. Focusing on the changes in point-of-view between executive agents and those they survey in these films, my analysis will ultimately show how genre cinema can serve as an invaluable mode of human rights critique of practices that expand the surveillance power of the state. These self-contested films engender a new perspective upon the gaolers of this panopiticon while revealing the humanity of the prisoners of this border setting, so often lost in law and within the public discourse.

Art and Critical Research

The art of questioning military surveillance optics

Rune Saugmann, rune.saugmann@uta.fi, University of Tampere

This paper uses the art photography of Richard Mosse as a tool with which to question how militarized forms of seeing distinguish between peace and conflict in war zones. New developments in militarized seeing are at the heart of debates over precision warfare from drone strikes to close air support. Producers and users simultaneously tout the optical precision of systems of militarized systems and attribute occasional failures of these systems to a fog of war. In this paper I use the photography of Mosse to engage such militarized forms of seeing. Nearly three decades ago visual culture theorist Hal Foster formulated the problem for scholarship in a world of visual representations as one of investigating not only 'how we see, how we are able, allowed, or made to see' but also 'how we see this seeing or the un-seen therein'. (Foster 1988:ix). Taking this concern to military seeing, the work Mosse – which uses the now-outdated Kodak Aerochrome military surveillance film which aims to reveal what is invisible to the naked eye - can be used to think about the regimes of visibility in militarized seeing and to question the un-seen in systems of militarized optics promising to see further than the human eye.

What can Robocop(s) teach to critical security studies? An "amateur" reading of surveillance, (dis)order, and critique

Rocco Bellanova, rocco@prio.no, PRIO - Peace Research Institute Oslo

Harry Potter, Battlestar Galactica, zombies and other popular culture 'products' are no longer bizarre objects of research. Still, the attention mostly focuses on their role as representations of something out-there. Their potential agency may be recognized in relation to high and low politics, but there is little interest in their ability to challenge and complement researchers' representations and methods. In this contribution I argue in favor of charting the multiple ways in which popular culture advances its own framing of politics. The aim is not only to understand how specific products support or question security practices, but also how a popular culture experience can originally contribute to critical security studies. I engage with two Robocop films (1987 and 2014). I claim no expertise in cinema studies: I rather adopt an "amateur" perspective (to quote Rancière). Through a back and forth between my story as researcher and as spectator, I re-engage with these two movies in relation

the following themes: surveillance, (dis)order, and critique. I present the security practices and the strategies of description adopted in the movies. Then, I juxtapose Robocop(s) to my experience of critical security studies and surveillance studies, highlighting what, and how, we may learn as spectators of popular culture.

Can you hear it too? Looking into surveillance through sound and music

Gloria Gonzalez Fuster, gloria.gonzalez.fuster@vub.ac.be, Vrije Universiteit Brussel (VUB), Research Group on Law Science Technology & Society (LSTS)

Our understanding of surveillance is marked by the notions of visibility and invisibility, epitomised by images such as the secret watchful eye or Big Borther's gaze, and defined by concepts like the Pan(syn)opticon and sous-veillance. Emphasis on the interplay between the visible and invisible, however, can neglect the significance of the different modes in which these operate, leaving in the dark important insights on surveillance's functioning and power. This contribution will move beyond such conceptions by exploring surveillance via the 'paranoid ear', to quote Seth Cluett: it will review and critically discuss the possible ways in which surveillance might be sonically approached and unpacked. First, it will consider existing accounts of (popular) music on surveillance (including the seminal work by Gary T. Marx), and note how these can be expanded to include not only other -less popular and more diverse- pieces of music, but also to encompass sound art and revealing experiences such as, for instance, Christina Kubisch's electrical city walks. Second, it will put forward an alternative approach to apprehending the relationship between sound, music and surveillance built on their technological nexus, through the acknowledgement of the intertwined histories – as embodied, for example, by Lev Sergueïevitch Termen's inventions. Third, it will question the validity of thinking (modern) music as surveillance, supported by Theodor W. Adorno's sociological critique and Jacques Attali's 1970s portrayal of the evolution of the contemporary music industry. In this context, it will consider both the disciplinary potential of music and sound, on the one hand, and specific practices of surveillance through (digital) musical consumption, on the other. Finally, the paper will examine the added value of the described sonic perspectives for surveillance's study and contestation.

Consolidating the Commercial: The Digital Politics of ISIS Recruitment Videos

Anna Leander, ale.mpp@cbs.dk, CBS MPP

This article explores the politics of digital videos. More specifically it looks at the recruitment videos through which Westerners are explicitly invited to join the ISIS. The article argues that to understand the politics of these videos requires a better understanding of "visual language". To this end, it introduces the distinction between visual and visible and suggests conceptualizing the politics of videos in terms of the regimes of visibility. The article further suggests that digitization has consequences for the aesthetics and the circulation re-produced through the regime of visibility. Digitization makes juxtapositions of texts core to aesthetics and contagion central for circulation. Analysing the ISIS recruitment videos on this basis, brings out the extent to which these videos consolidate the role of the commercial in the regime of visibility. Commercial text is not merely one text among the many that are juxtaposed in the videos. It embeds them all. Similarly, the commercial is not simply one of many rationales invoked in efforts to shape and control the circulation of the videos. It is inscribed into the infrastructure through which the circulation takes place. Politically this is important and discomforting. It signals a potential for political engagement. However, in so doing it is also discomforting. It shows that the political barriers between ISIS and the West may be more porous than either side would like to acknowledge.

Mobility

From Lifestyles to Locations: Situating mobile analytics within the political economy of consumer surveillance

Harrison Smith, harrison.smith@mail.utoronto.ca, University of Toronto

Audience segmentation and marketing has come to increasingly rely on mobile surveillance infrastructures to create new forms of segmentation, analysis, and influence through the collection, storage, and analysis of location data and mobility patterns. This has been made possible through a complex of social, economic and technological forces, particularly the rise of smartphone geo-spatial media, as well as the layering of various kinds of sensors throughout the urban environment. This also includes the need to understand mobile analytics within a larger political economy of consumer

surveillance, particularly as older methods of social media surveillance are increasingly questioned with respect to epistemological beliefs of reliability and validity, as well as political and economic issues around authority, trust, and consent in enacting these kinds of techniques of surveillance and influence. This paper will present findings from the author's doctoral research that investigates the institutional goals, and ethnomethodological beliefs of mobile analytics companies that use location data to target and influence consumer behaviour. Data realized from semi-structured qualitative interviews from a range of participants in the digital, mobile, and location based marketing industries, including entrepreneurs, CEOs, data scientists, media strategists, digital ethnographers, and marketing consultants in order to understand the commodification and use value of location data will be presented in order to critically examine the underlying political, economic, and cultural dimensions of mobile consumer surveillance and audience segmentation practices.

"I would trust the system more, but my car less." Trust, Privacy and Surveillance in the age of the Driverless Car.

George Filip, George.Filip@nottingham.ac.uk, The University of Nottingham

Xiaolin Meng, Xiaolin.Meng@nottingham.ac.uk, The University of Nottingham

In the context of ubiquitous data collection and analysis, surveillance of the individual and sharing personal information have started playing an increasingly important part in the future of the transportation industry. With new emerging technologies such as the driverless car and the Vehicle-to-Anything (V2X) communications (the connectivity between the vehicle and everything else surrounding it), the information that the vehicle is collecting and sharing with other connected-smart objects, plays an important role in the successful implementation of such systems. Nowadays, car manufacturers as well as research institutions are looking into creating a viable driverless vehicle, capable of working either independently or by connecting with the others, and thus becoming a part of the Internet of Things (IoT). The driverless car is the subject of substantial research in different areas. However, the role of privacy and surveillance has only recently been under the spotlight. In a recent interview, a BMW executive has drawn the public's attention towards the interest expressed by marketing companies that wish to gain access to the data collected by the sensors of a driverless vehicle, which have an important cost on the privacy of users. Another example of how sensitive information such as location has been unethically used is given by the scandal in which TomTom has sold the GPS data of drivers to the enforcement agencies, in order for them to find out where to set

up speed cameras. Further attention was later drawn by a Ford executive when he stated: “We know everyone who breaks the law, we know when you're doing it. We have GPS in your car, so we know what you're doing”. For reasons such as these, recent studies are trying to address the problem of collecting and sharing private information before the actual mass production of the connected driverless car. This research paper will look into the ethical perspectives of collecting and sharing private data of the individual, in the V2X context, as well as into the effects of this sharing of information on the individual trust in such systems and their willingness of using them. In order to address these issues and offer an informed perspective, a critical literature review was conducted which was later on followed by deploying a survey that, among others, tried to grasp the importance and effects that collecting and sharing of information (such as location, direction, speed) has on intended users’ trust. 291 participants responded to the survey questions that were addressed on the theme of collecting and sharing of data with a further 256 filling in the open ended question that asked them to state what would the effects of collecting and sharing information would have on their levels of trust. Following the thematic analysis of the open ended question, a series of themes related to surveillance, fear of hacking as well as benefits that the connectivity would bring (among others), in relation to the trust of the users, will be presented and discussed.

Mobility and Visibility

An Investigation into the Surveillance Potentials of Autonomous Technologies: Visibility, Ubiquitous Embedded Surveillance and Mobility

Jennie Day, 0jad8@queensu.ca, Queen's University

Autonomous technologies are becoming increasingly prevalent within society, providing potential solutions to a variety of social, political and economical challenges. Common unintended consequences or byproducts of uncritical integration of novel technologies into society, however, are the surveillance potentials of these celebrated technologies and the degree to which they are bearers of surveillance data (Lyon 2007; Lyon 2015). The moving surveillance platforms of Unmanned Aerial Vehicles (UAVs) and autonomous vehicles are examples of the vanishing yet ubiquitous characteristic of contemporary surveillance, as surveillance is increasingly woven and embedded into the technologies, infrastructures, systems and practices of everyday life [Murakami Wood 2014; Lyon 2015]. Whist visibility of surveillance devices is decreasing, the lives of surveillance subjects

are becoming more transparent through the black-box processes and consequences of dataveillance. Through an analysis of illustrative case studies of UAV use in the UK, USA and Canada, an exploration of the surveillance capabilities and implications of emerging autonomous technologies could contribute to the debate concerning how to effectively integrate technology into society through the modification and/or creation of policies, regulations and laws. Questions relating to the emergence and integration of these autonomous systems such as “since many aspects of today’s surveillance society are increasingly reliant on the capture, retention and analysis of as much data as possible, how might the collection of finely grained, space-time data by autonomous vehicles (which is intimately tied to the function of automated mobility) have surveillance implications for the ‘actionable intelligence’ of the data in many spheres of society, specifically the Smart City (Andrejevic 2014)?”,“what civil liberty and human rights issues are raised by autonomous technologies?”, and “how may these emerging systems of surveillance bring about new modes of power, implicate democratic participation, and shift how members of society relate to each other, and to the new technology?” are explored.

Hawk Eye View: Shifting the Surveillant Gaze

Stéfy McKnight, stefy.mcknight@queensu.ca, Queen's University

Hawk Eye View (2015) is an exhibition that looks at the history of third party surveillance in North America. Considering Snowden’s revelations (2013), Hawk Eye View explicitly looks at NSA and CSIS sites through Google Earth imagery. Google is eminent for providing users access to maps and detailed images of geographical spaces. Google Maps and Earth retrieve user metadata via GPS, direction searches and IP addresses. In 1998, section 215 & 702 of FISA ordered for third parties to turn over evidence and data if the government saw it relevant to investigation. Section 215 was revisited after the War on Terror, in 2005. Similarly in 2015, Prime-Minister Stephen Harper has proposed to implement a new anti-terrorist bill of similar nature, C-51. By looking at Five Eyes it is evident that Canada and the United-States’ surveillance plans are inextricably linked to one another. My artist talk looks at the ways that Google Earth and Maps reinstate some of the ways that the Canadian and US government acquire metadata to politically ensure a survival state. The overall theme of this exhibition is revealing concealed spaces. Hawk Eye View is an assortment of installations: wallpaper, ‘maquettes’, banners and prints of NSA and CSIS headquarters. Interactively, viewers will load information and addresses of the intelligence sites using a QRcode reader on their mobile device. The surveillance gaze shifts by giving viewers the tools to observe the

institutions that are normally doing the 'surveilling'. This talk will look at the methodologies, creation process and ways that HEV critiques and engages with third party surveillance in North America. In addition, I will look at the benefits and importance of research creation when focusing on themes of looking.

On the Buses - Surveillance and Everyday Mobility

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

This submission considers the use of surveillance on Britain's public buses. In particular, the paper argues that while the use of CCTV and other supervisory systems has risen exponentially since the late nineteen-nineties (validated by the identification of the 7/7 bombers in recent times), that surveillance has always played a significant role in the commuter's journey. In today's context, public transport systems define the most sublime platforms for thinking about surveillance mobilities - in other words, as the movement of peripatetic populations, and the ability of transit systems to record, permit or deny passage, and otherwise scrutinize commuters during all aspects of their journey. However, on an increasing scale, the notion of mobility equates to the movement of surveillance systems themselves (whether mounted to public officials or their vehicles), and even to the fusion of both state and corporate surveillance via mutual access points. This paper argues that public transport networks have become the point in which the population, law enforcement agencies and the private sector engage - drawing together synergies between risk management, criminal prosecution, litigation suits, passenger comfort and safety, and corporate efficiency. Under this cavalcade of themes, up to 15 forms of surveillance can be enacted in any one vehicle. These range from CCTV (fore, aft, side-mounted, facial recognition, passenger counting, infra-red, 360 degree, tamper proof cameras, and live wireless CCTV streams), to CCTV feeds inside the buses, Wi-Fi for passenger use, voice recording technology, travel cards, GPS position tracking, DNA swab kits, and the traditional bus conductor. Today, public buses represent the epitome for how surveillance is mobilized in modern society, though their history in this context dates back to the 1850's. The paper therefore questions how novel the concept of mobile surveillance is, but equally aims to reinvigorate the debate and call for a new examination of surveillance mobilities.