SSN 2022 Rotterdam session streams:

9th Surveillance Studies Network Conference 2022

Rotterdam

STREAM 1: ART & CULTURE
STREAM 2: HISTORY & RELIGION
STREAM 3: LAW & JUSTICE
STREAM 4: SECURITY & POLICING
STREAM 5: POLITICAL ECONOMY
STREAM 6: MEDIA & COMMUNICATIONS
STREAM 7: SOCIETY & INSTITUTIONS
STREAM 8: TECHNOLOGIES
STREAM 9: THEORY

Day 0: Tuesday, May 31 2022

Prachtig Rotterdam (Willemsplein 77, 3016DR)

Official Welcome Reception (19:30 - 21:30)

Day 1: Wednesday, June 01, 2022

Session	Forumzaal / Zoom 1	T3-06 / Zoom 2	T3-21 / Zoom 3	M2-11	M2-12	T3-35
Registration (starting at 8:30 in Van der Goot (M) building, 3rd floor)						
1 (8:45 – 10:00)	*Human Rights (1): Asia*	*Data Sharing & Supply Chains*	*Crisis, Vision & Privacy*	*Artificial Intelligence*	*Panel: Digital Technologies in Policing and Security (1)*	
2 (10:00 – 11:30)	*Human Rights (3): MENA*	*Faces & Face Recognition Tech*	*Social Media*	*Counter-terrorism (1)*	*Police & Intelligence*	*Bodies & Tracking & Education (1)*
Coffee Break (11:30 – 11:45)						
PLENARY: Welcome, Prizes & KEYNOTE 1: Simone Browne (11:45 – 13:15 in Forumzaal)						
Lunch (13:15 – 14:30)						
3 (14:30 – 16:00)	**Panel: BOLD Cities (1)*	*Panel: Surveillance & Subjecthood*	*Film & Games*	*Counter-terrorism (2)*	*Policing Technologies*	*Contested Technologies*
Coffee Break (16:00 – 16:30)						
4 (16:30 – 18:00)	*Social Relations and Capitalism (1)*	*Panel: Reconsidering the Trace – Alternative Surveillant Epistemologies*	*Education (2)*	*Panel: Privacy Studies, Surveillance Law*	*Human Rights (2): Russia*	*Nature & Sustainability*
Close at 18:00						

Day 2: Thursday, June 02 2022

Session	Forumzaal / Zoom 1	T3-13 / Zoom 2	M1-16 / Zoom 3	M2-11
Registration (starting at 8:30 in Van der Goot (M) building, 3rd floor)				
5 (8:45 – 10:00)	*Housing*	*Platforms*	*Design & Coding*	*Data Justice*
6 (10:00 – 11:15)	*Public Health & COVID-19 (1)*	*Intelligence & National Security*	*Algorithms*	*Privacy Law*
Coffee Break (11:15 – 11:30)				
7 (11:30 – 13:00)	*Public Health & COVID-19 (2)*	*Subjectivities and Workplaces*	*Human Rights (4) China*	*Visual Art & Performance (1)*

Lunch (13:00 – 14:15)

PLENARY: ARTS PRIZE & PANEL (14:15 – 15:15 in Forumzaal)

	Forumzaal / Zoom 1	T3-10 / Zoom 2	T3-06 / Zoom 3	M2-12	M2-11	T3-39
8 (15:15 – 16:45)	**Panel: BOLD Cities (2)*	*Vigilantism & Community Surveillance*	*Visual Art & Performance (2)*	*Panel: Surveillance Studies and the Global South*	*Panel: Digital Technologies in Policing and Security (2)*	*Policing & Cameras*

Coffee Break (16:45 - 17:00)

PLENARY: KEYNOTE 2: Elizabeth Joh (17:00 - 18:00 in Forumzaal)

20 Years of Surveillance & Society Reception (19:00 - 21:00) - **Arminus (Museumpark 3, 3015 CB)**

Day 3: Friday, June 03, 2022

Session	Forumzaal / Zoom 1	T3-17 / Zoom 2	T3-25 / Zoom 3	T3-31
Registration (starting at 8:30 in Van der Goot (M) building, 3rd floor)				
9 (8:45 – 10:00)	*Borders & Migration (1)*	*Conflict*	*Technological Imaginaries*	*Panel: Surveillance & BWCs*
10 (10:00 – 11:15)	*Borders & Migration (2)*	*Education (3)*	*History (1)*	*Law & Technology*
Coffee Break (11:15 – 11:30)				
11 (11:30 – 13:00)	*Social Relations (2)*	*History (2)*	*Borders & Migration (3)*	*Human Rights (5): Europe & Global South*

Lunch (13:00 – 14:15)

Distinguished Contribution Award (14:15 - 15:15 in Forumzaal)

	Forumzaal / Zoom 1	T3-17 / Zoom 2	T3-16 / Zoom 3
12 (15:15 – 16:30)	**Panel: AIPact*	*Rights & Resistance*	*Panel: Predictive Policing*
Coffee Break (16:30 – 16:45)			
13 (16:45 – 18:15)	*Panel: Researching the Rise of Employee Monitoring Applications*	*Public Attitudes, Influence & Information*	*Panel: Affective Surveillance through Emotional AI in Smart Cities*

Close at 18:30

STREAM 1: ART & CULTURE

Film & Games

Moderator: Fieke Jansen

Fareed Ben-Youssef, Kiyoshi Murata and Andrew Adams:

‘Capturing the Trap in the Seemingly Free: Cinema and the Deceptive Machinations of Surveillance Capitalism’

Shoshana Zuboff's Big Other concept captures the paradigm shifts provoked by surveillance capitalism and its seemingly free services. The Big Other brings with it “new possibilities of subjugation... as this innovative institutional logic thrives on unexpected and illegible mechanisms of extraction and control that exile persons from their own behavior.” Our paper disrupts the Big Other’s pervasive illegibility by comparing three examples of global cinema. In the process, we fill in historical blind spots in Zuboff's framework. To underline the Big Other’s new subjugations, our interdisciplinary paper traces the line between what constitutes just and the unjust surveillance within business. Our examples feature both enthused surveillance capitalists as in James Ponsoldt’s adaptation of "The Circle" (2017) as well as confused, even terrified end users in Kiyoshi Kurosawa’s horror film "Pulse" (2001). We then frame the historical roots of such mass surveillance by situating studies on Big Data’s role in the Holocaust against Quentin Tarantino's WWII film "Inglourious Basterds" (2009). Our comparisons illustrate the consequences of the Big Other's emergence: to be reduced to data is to accept the possibility of being deleted. Ultimately, these films give surveillance and information ethics scholars a new language to map out surveillance capitalism’s trap.

Hugo Ljungbäck:

‘Bringing the Drone Home: Resisting Empty Metal’s Surveillant Gaze'

Spider-Man: Far From Home (2019) is just one of many recent blockbusters to manifest the West’s anxiety about unmanned aerial vehicles (UAVs) and other drone technologies turning on and/or being used against a “first-world” population. “Far from home” is exactly where the war on terror has been fought for the past fifteen years. On the contrary, for the past decade, artists and filmmakers beyond mainstream cinema have sought ways to problematize drone warfare through their creative practices, challenging military surveillance and violence by appropriating, parodying, and turning the drone’s military gaze back at itself (or onto Western populations). In Adam Khalil’s and Bayley Sweitzer’s Empty Metal (2018), the filmmakers imagine a dystopian future in which the police state turns its surveilling eye onto its own political and ethnic minorities. By “bringing the drone home,” the film’s narrative proposes that the five ideological groups it represents—a punk band, an indigenous family, a Rastafarian hacker, a Buddhist hermit, and a secret militia—all face a common enemy in the violent state apparatus. In my presentation, I will explore how Khalil and Sweitzer tease out the connective tissue between dystopic state surveillance, police brutality, and racialized oppression. I argue that, by aligning their counter-narrative of political radicalization, citizen action, and sousveillance with a utopian “politics of affiliation,” the filmmakers raise key questions about sovereignty, autonomy, and citizenship in the surveillance state. “And all the while, the drones are watching…”

Greg Elmer and Stephen Neville:

‘The Silent Sounds of Incarceration: Gamified Escape and Media Scarcity'

In this paper we develop a hybrid app walkthrough and soundwalk method to conduct a case study of a prison escape game on the Amazon Alexa platform. The game is an example of an invisible app that sonically mediates a carceral-surveillant environment for purposes of entertainment: curiously, the game does not realistically represent any audile symbols of prison life but instead silences these traces in favour of a ‘family-friendly’ experience. The goal of our paper is to further develop a conceptual framework of “media scarcity” (Elmer 2020) that speaks to the conference’s key track of sensing beyond seeing. In an effort at countering the predominate media abundance theory that posits “rich choice” and visuality as the prevailing media logic, our study of the prison or detainment cell as a media sparse space, and its inhabitants as living largely media scarce lives, raises important questions about the capacity and manner in which such communities can narrativize their carceral lives and pasts. We argue through our case study that technocultural escapism serves to compound political problems of media scarcity for incarcerated people. Our paper asks: How does a lack of self-representation and mediated misrepresentation of carceral environments challenge reforms efforts that imagine futures of decarceration?

Visual Art & Performance (1)

Moderator: Jonas Breuer

Mehdi Ghassemi:

‘Aesthetics and Politics of the Extimate Gaze: Reading Surveillance Street Art with Jacques Lacan'

As surveillance cameras have become increasingly ubiquitous in our urban space, much of “surveillance street art” primarily deals with visual surveillance, especially with the aesthetic quality of “the surveillance society” and the types of “visual landscapes” that surveillance has generated through the recent years (Andrea Brighenti 2010). More specifically, adds Brighenti en passant, these artists explore the “uncanny” sensation of being watched by an artificial eye. This paper argues, however, that there is much more at stake in surveillance art’s engagement with the uncanny gaze of the panoptic Other. I rely on Jacques Lacan’s key reworking of the Freudian uncanny as “extimity” to examine the ways in which the panoptic gaze intrudes in the individual’s sphere of privacy by blurring the boundaries of the human subject itself. I will then use his notion of the objet a to look at the aesthetic gestures employed by surveillance street artists to responds to this intrusion. My claim here is that these artists question the totalizing claim of the gazing Other by challenging its presumed ontological completeness, by laying bare its inherent contradictions, and revealing its points of impossibility. Finally, I will explore the political dimensions of these aesthetic engagements and how they fit in the wider context of power relations in our contemporary digital surveillance societies.

Jaseff Raziel Yauri-Miranda and Victoria Catalán Ascaso:

'Stalk me to the end of love': Performing intimacy and affections in hyper-surveilled digital spaces'

This presentation draws from two artistic research projects of social experimentation in the digital world. They question affections and interpersonal relationships constructed through the mediation of technological devices. "Stalk me to the end of love", is based on the creation of an application for smartphones, proposing a hyper-surveillance space among equals that appropriates the mechanics used by dating applications such as Tinder, Lovoo, and OkCupid. The application connects two users anonymously and randomly through images they share. It generates a mutual admiration bound, an open window to the intimate space in which it is only possible to interact via images. It questions visibility based on the gaze and allows someone to admire and be admired by a single person each time. "ToDo LoVe Club" is a 'ritual' of cyborg love for hybrid, mutants and perpetual cybernetic beings. It is a participatory performance based on speed dating. Here,dates are not held face to face, but using participants' mobile phones in a controlled space in which strangers allow other strangers to access their devices for five minutes. The proposal seeks to experience and oversee the mutations that technological devices generate in our experience of anonymity, identity and intimacy. The projects are conducted using questionaries in a random sample of people from different social backgrounds in the city of Bilbao. With the collaboration of a computer science team, both the application and the mechanics of the projects have already been tested in a preliminary sample and are ready to be replicated. Each proposal is conducted with the consent of each participant who remains anonymous and in accordance with personal data protection and intimacy rights.

Stéfy Mcknight and Julia Chan:

'"Cam Hunters": Hidden Cameras, "the New Normal," and Satirical Performance'

HOW TO PROTECT YOURSELF FROM HIDDEN CAMERAS IN YOUR AIRBNB :

- Look for bad reviews of the property
- "[D]iscuss the use of surveillance devices using Airbnb's messaging feature"
- Examine out-of-place items
- Check for one-way mirrors
- Use a flashlight to detect lenses
- Use a thermal camera or radio frequency reader

- Run a script to disable wifi cameras
- Hire a surveillance professional to do a sweep

“[S]pending 15 minutes or so upon check in hunting around your rental should probably be the new normal,” recommends Mashable.com.
In this paper, we will present and discuss our satirical video “Cam Hunters” (9 mins). Drawing reference from artists such as Hito Steyerl and Jill Magid, our “instructional video” critically interrogates these suggested methods of “self-protection” within the context of neoliberal individualized responsibilization. As surveillance of this kind is “an emotional event” (Koskela 300), our project seeks to respond to and subvert the affect of surveillance creep – or what Mashable referred to as “the new normal.” Our video and presentation explore questions of privacy, (economic) access, responsibility/risk, and surveillance culture through creative experimentation with these methods of self-protection.
The “Cam Hunters” video is part of a larger collaborative performance project between Drs. Stéfy McKnight (STÉFY) and Julia Chan, which satirizes and criticizes surveillance creep in personal and private spaces. The video can be viewed at camhunters.org.

Hille Koskela:

‘Empowering exhibitionism in surveillance art'

Surveillance art projects commonly aims at showing how digital technologies can be misappropriated and how they endanger people’s right to privacy. In this presentation, I will look at art from a different angle: contemporary surveillance art is created to critique or oppose surveillance policies and regimes. Art provides a way to tackle surveillance related issues creatively. Artistic and playful representations widen academic understanding of the nature and extent of subjective surveillance experiences as well as the political context of surveillance.
My presentation will be based on the works of three artists:
-Dana Dal Bo (focusing on surveillance practices, reality television, re-enactments, the supernatural and the posthuman)
-Juno Calypso (studying solitude, desire and femininity through a dark comedy lens)
-Frank Schallmaier (focusing on nude or scantly-clad selfies of gay men collected from the social media, faces hidden with flashes).
I will explore issues related to body, objectification, self-esteem, voyeurism, exhibitionism, narcissism, and self-surveillance in order to understand how popular culture and social media influence the re/de/construction of gender identity and sexuality.

Visual Art & Performance (2)

Moderator: Julia Chan

Susan Cahill:

‘Surveillance Frontierism: Art and the colonial project of surveillance'

My presentation focuses on a new research project that examines art and creative practice in the context of what I am calling “surveillance frontierism.” The concept of “surveillance frontierism” seeks to analyze expansive projects of Canadian security and surveillance through their reciprocity with ongoing histories of colonial capitalism, which include white supremacy, resource extraction, and technological innovation as salvation. My interest here is to connect contemporary surveillance with the histories of the settlement of the land. To develop this concept in my paper, I focus on a series of contemporary creative artworks that work to “unmap” the Canadian settler state as part of the decolonial project of complicating the relationship and role of surveillance in histories of colonial-capital extraction. Through this work, I situate art production as a specific methodology that is uniquely positioned to generate new ways of seeing these histories and to imagine new possible futurities.

Karen Louise and Grova Søilen:

‘A Sense of Ambient Entrapment in Hito Steyerl's Factory of the Sun’’

This paper investigates how artworks may reflect, react to, and produce the way we see and feel surveillance now in ways comparable to what Raymond Williams once termed ‘structures of feeling’. Through a reading of Hito Steyerl’s immersive video installation environment Factory of the Sun (2015), the paper proposes that the artwork generates an affective experience of surveillance which can be identified as a sense of ambient entrapment. Inside the dark installation space, visitors are immersed in a blue LED grid environment and encouraged to recline in beach chairs facing a large screen. What is perceptible as time passes inside Factory of the Sun, the paper argues, is a vague, yet pervasive feeling of a controlled environment saturated by surveillance and exploitation, where machine perception and algorithmic processes are hard at work. The sense of ambient entrapment produced by the artwork is a vague sense of something working and conditioning in the background, of technologies extracting and exploiting personal data, while we at the same time desire and feel the lure of the said technologies and devices. The paper concludes that we should turn to contemporary art as sites of knowledge of the experience of surveillance of the present moment.

Molly Roy:

‘Choreographing Countermaps: Space, Safety, and Jennifer Harge’s FEDS WATCHING'

In 2018, Detroit-based dancer and choreographer Jennifer Harge, Artistic Director of Harge Dance Stories, staged a new work entitled FEDS WATCHING, an encoded refute and embodied subversion of the targeted surveillance of Blackness. Activating tactics of Black fugitivity and gesturing towards the labors of domestic geopolitics, the piece generates a site of what Simone Browne has termed dark sousveillance, an oppositional countersurveillance practice that enables and imagines alternate paths and ways to exist and move in the world. Concurrent with this insurgent choreography, and structuring the shared material space of Detroit, is Project Green Light, a partnership that joins privately-owned and operated CCTV cameras with the networks of the Detroit Police Department, constituting an experiential map of public space rooted in racialized, ubiquitous surveillance. In this paper, I position and analyze FEDS WATCHING and Project Green Light alongside one another, examining how embodied creative practices can inform and enliven understandings of surveillant infrastructure and its corporeal and affective implications. I argue that Harge's choreography mobilizes a process of reclamation and respatialization, tracing an aperture through which to disrupt relations of power and destabilize the topography of (dis)belonging that constructs surveillance space.

Stephanie Brown:

'Suffrage Journalism as Surveillance Art, 1913'

This paper traces women's historical resistance to state surveillance that can be found in the pro-suffrage British newspapers Votes for Women and The Suffragette. These papers mobilized images of suffragists being forcibly fed in prison against the British Government and its surveillance apparatus, bringing the practice out of the inaccessible space of the prison and into the public imagination. Following Torin Monahan's suggestion that surveillance art can "destabilize viewers and suggest possibilities for resolution or containment…through recognition of complicity and collective responsibility," I argue that these images invoke the possibility that militant action might prevent further such violations, and that this possibility was crucial to their purpose as militant recruiting tools. These torturous images' claims about the state's use of force work to destabilize that viewer's relation to their prior political beliefs. They suggest that if the viewer is made uncomfortable by their own instinctive responses or social positioning—if they do not wish to be either voyeur or bystander—suffrage militancy offers opportunities to productively reorient that response. This reorientation requires the viewer to reject the role of surveillor and become wary of how surveillance and surveillant looking are imbricated with carceral, medical, and legal systems.

STREAM 2: HISTORY & RELIGION

History (1)

Moderator: Balázs Prokk

Cristina Plamadeala:

'Recruitment of Securitate Informers in Communist Romania: psuchegraphies in Securitate files'

This paper proposes to examine the concept of psuchegraphy and how it relates to the study of Securitate archives as well as methods of recruitment of Securitate informers. Psuchegraphy is a type of life scrutiny and rewriting that involves collecting biographical data on someone that provides sufficient clues about a person's vulnerabilities, core beliefs, character, and identity, or, to use the language of ancient Greeks, about a person's psuche (ψυχή). Psuchegraphy is a precursor to recruitment and many individuals can be successfully manipulated by this method because it seeks to jeopardize that which is considered of most importance to a human being (Plamadeala 2019a, 2019b). In this paper, I explain the four stages of constructing a psuchegraphy on a target, as described in Securitate instructive manuals and teaching materials on how to acquire recruits. These teaching materials were used by Securitate officers in their professional training and during their employment for the Securitate. Using examples from Securitate files, I show that four stages of doing psuchegraphic work were: 1) identification of potential candidates (punctarea candidaților); 2) study and background check of potential candidates; 3) selection of candidates; 4) recruitment of selected candidates. The paper is based primarily on research conducted in Securitate archives, currently stored at the Council for the Study of Securitate Archives in Bucharest, Romania.

Cliodhna Pierce:

'Examining the impact of surveillance on societal interactions with state institutions. Comparing NI and GDR During the 70's and 80's'

Surveillance is a form of power and control that has a direct bearing on how we live our lives, interact in our communities and participate in our political systems. As Micheal Foucault suggests, 'Freedom disappears everywhere power is exercised'. This is most often at the expense of the individual because state institutions prioritise security: 'The state is envisioned as a kind of political power which ignores individuals' (Foucault, 1982, p.782). The political and societal impact of surveillance has a direct bearing on our relationship with the political system and this in turn affects our attitude to how we interact and engage with government institutions. As David Lyon point out in his work on Surveillance After September 11 "Surveillance has become a routine and mundane feature that is embedded in every aspect of life and operates in a wide range of agencies well beyond the confines of central state" (Lyon, 2001). With the increasing use of surveillance techniques in modern security and policing strategy, the state's control over these intuitions appears to have grown, unlike the case of East Germany and Northern Ireland; however, it can be said that this power does not appear to be conducted to the same extent in contemporary society. As Foucault observes:

> It is certain that in contemporary societies the state is not simply one of the forms or specific situations of the exercise of power--even if it is the most important-but that in a certain way all other forms of power relation must refer to it this is not because they are derived from it; it is rather because power relations have come more and more under state control (although this state control has not taken the same form in pedagogical, judicial, economic, or family systems). (Foucault, 1982, p.793)

Despite the ever-increasing intrusions into the private sphere via new invasive technologies and laws, the impact these have on the way we function as a society remains unclear. In a surveillance state, the control exerted upon citizens often forces them into becoming compliant with policies and actions that under a free system would be opposed. This has a chilling effect on socially beneficial behaviour, which results in deterioration of our interaction with state institutions, hampering our ability to vocalise any concerns on the way our state is governed. This paper will use East Germany and Northern Ireland during the 70's and 80's as historical case studies of surveillance societies, examining the impact and role surveillance operations plays on societal interactions with state institutions.

Delano Aragao Vaz:

‘Ego suspecto: colonialism, surveillance, and the creation of “the other”'

This paper advances the concept of ego suspecto (I suspect/am suspecting) as a development of Descartes’ ego cogito through the colonial encounter. Underlying present-day surveillance practices, the ego suspecto automatically gazes at the racialised Other as a suspect constantly “out of place” and thus a justified target for more pervasive and invasive forms of surveillance. Building on Anibal Quijano’s concept of coloniality and Simone Browne’s argument that prototypical whiteness relies upon dark matter for its own meaning, this paper contends that surveillance plays a crucial role in (re)creating racial hierarchies. Through a genealogical account, I trace some of the ways that European settlers constituted themselves and “the other” in “racial” terms. I argue that, by understanding what lies underneath the European mentality that crossed the Atlantic and confronted the “other face”, the connection between modern racism, surveillance, and the dawn of what we now know as the Americas becomes evident. I demonstrate that race and racialising processes are covered by an aura of suspicion in such a way that both concepts of race and suspicion are conflated in their essence. Thus, the ego suspecto mentality construe the essence of the racialised body as suspicious, naturalising it as a surveillance target.

Gavin Smith, Mark Andrejevic, Chris O'Neill, Neil Selwyn and Xin Gu:

‘The Emerging Inter/Face: theorising the rise and bodily impacts of facial recognition technology'

As progressively more interactions and transactions occur remotely through the agentive mediums of digital technologies and data, so distanciated actors require to be individuated and made accountable by the software infrastructures responsible for hosting the activity. This is especially the case when the platform being accessed is a government or financial service, and where the management of fraud risks and artifice have come to be key concerns. As a governmental response to what has been framed as the problems of anonymity, insecurity and duplicity in the mobile and risk-infused world of the contemporary period, biometric technologies have been introduced which have the capability to anchor the identity of individuals to the fleshy materiality and morphology of the body. These ‘recognition’ technologies focus on measuring different parts of the body – the retina, the fingerprint, the voice, the face – and rendering each into a machine-readable code so that they can be scanned and their accuracy matched with virtual referents contained within databases. Of these biometric authentication tools, the use of facial recognition is one application that is growing in scale and prevalence, as a means of both verifying identity claims for access control (e.g. Apple Face ID) but also identifying individuals in real time or retrospectively as they transit through public space (e.g. smart CCTV cameras). Drawing on discourse analysis and interviews with key stakeholders in the Australian face recognition industry, this paper offers a conceptualisation of how the biometricised face is becoming akin to a unifying, machinic interface. Faces, we argue, double up as bodily borders of the self and as biopolitical borders of the institution: sites on which a set of governmental and economic regimes are being projected, leveraged and realised. Beyond concerns with privacy, liberty and discrimination, we point to some of the major social and embodied implications of having the face exhaustively tracked and inferentially profiled as it engages both actively and passively with different surveillance mechanisms. Crucially, we ask what forms of surveillance work these technologies perform and what types of micropolitical face work, to borrow Ervin Goffman's term, materialise when faces betray, occlude, fail, transform or become incompatible.

History (2)

Moderator: Cliodhna Pierce

Balázs Prokk:

Efficient Market-Democracy and Sick Normality: How the Logic of Surveillance Works in Decentralized Networks?

This paper is engaged to depict an underlying mechanism of subjectivity deformation in our neo- liberal age. Methodological individualism is the prominent approach for efficient policy-making; and it has a bottom-up way of thinking: from the individuals to the collective. To emphasize the downside effects of methodological individualism, I provide here an upside-down reflection, from the historical contexts of efficient governance to the modified understanding of rational subjectivity. During this paper I show how the demand for calculable predictability of the utilitarian tradition requires homogeneous and manipulable individuals. I conclude, that consumerism and choice- dependent rationality is a regression in the history of philosophy as emancipation. In order to depict these historical and essential correlation of rational choice and neo-liberalism, my research question is the following: How The Logic of Surveillance Works in Decentralized Networks?

Candace King:

'Phyllis Wheatley's Subversive Grammars: A Formative Blueprint for Sedition'

Through captivity, transport, and enslavement, Black women have endured and resisted the threat of surveillance. Although modern conceptions of surveillance history fail to capture the breadth of Black women's varied responses to domination, there is evidence of Black women's dissent as early as the 18th century. In this paper, I explore how Phyllis Wheatley single-handedly produced early and crucial documents of surveillance in the transatlantic slave trade and ingeniously engineered the blueprint for its subversion. As an enslaved African woman employed as a commodity for her master's entertainment, Wheatley produced poems under extreme levels of institutional supervision. Although literacy was illegal for enslaved women and men, Wheatley forged her own political agency with her pen using sharpened tactics of rebellion. In one of her poems, "On Being Brought from Africa to America" (1773), Wheatley executes a host of seditious rhetorical and poetic devices to expose the brutalities of captivity and contest the white, Christian gaze of her master. Utilizing Black Feminist Theory, I conduct a close literary analysis of Wheatley's poems to reveal formative grammars of subversion. In doing this, I expand the genealogies of surveillance through a re-examination of enslaved Black women's records of defiance in the 18th century.

Kathryn Blance:

'Racialised Surveillance in Historical and Contemporary Contexts'

Mobile phone footage of dangerous incidents between black individuals and police officers has become an increasingly common trend; perhaps peaking in 2020 when George Floyd's death was recorded and posted online. Indeed, as technologies have developed, there has been a rise in cases being filmed and distributed online. Much of the literature on this issue focuses on it being something of a modern phenomenon, rather than considering it as part of a continuum of racialized surveillance and control. Simone Browne's Dark Matters is the beginning of an urgent discussion on the history of racialized surveillance in America. This paper will look to continue this discussion by more explicitly widening the history of racialized surveillance with contemporary trends. Certainly, to understand contemporary America, and its landscape of surveillance, it is arguably important to step back in history. Since the days of slavery, surveillance has played a crucial role in the wider structures of control over the black population. Through the identification of technologies, such as slave bells and written slave passes, and the analysis of their specific sensory and affective dimensions, this paper will contend that the history of racialized surveillance has laid the foundations for contemporary racialized system of surveillance.

Zandi Sherman:

'Scanning and the Native Body: 100 Years of X-ray Technology at De Beers Diamond Mines'

For over a century the diamond mines of South Africa have used X-rays to scan workers for gems that have been swallowed or otherwise concealed using the body. This paper considers how this practice, which has exposed generations of diamond mine workers to unnecessary radiation, both produced and relied on racialised ideas of the black body. The X-ray has an inherently ambivalent relationship to the human body, it is championed for its life-saving potential, but is also capable of delivering life-threatening levels of radiation. Often narrated as an inherently medical technology, the X-ray has an equally long history of use for the non-medical surveillance of the human body. This paper tracks the history of X-ray scanning to consider how the technology's double life, as part of both medical and non-medical surveillance infrastructures, made it an ideal biopolitical technology, materialising the racially uneven distribution of life itself. In the late 19th century the swallowing of gems was explicitly narrated as a problem of the grotesque black body and the X-ray was celebrated as a technological fox. Contemporary practices of scanning are narrated in far more sanitised language but in fact this 19th century figure is still central to a calculus in which the security of the commodity justifies the exposure of workers to bodily harm.

Data Justice

Moderator: Bryce Newell

Jorge Pereira Campos and João Gonçalves:

'Data Donation Risk Framework: A New Avenue for Assessing E-Participation in Smart Cities'

This article advances a conceptual framework to understand how individuals construct the risks of participating in the co-production of services in a smart city by donating their data. It also offers the first documented conceptualisation of data donation. While there are multiple efforts to understand and regulate the relationship between citizens and data users, these still place an emphasis on consent and assume a lack of citizens' involvement with the entity handling their data. However, in the domain of smart cities, but also in fields such as research and software development, we see a shift to the understudied and ill-defined practice of data donation, which implies rethinking data dynamics and the associated risks. To address the need for a new way to think, act, and regulate data and privacy, we suggest the Data Donation Risk Framework (DDRF). We argue that constructions of risk emerge from an interplay of discourses that encompass perceived risks of traditional donation and risks specific to privacy. We suggest test cases for this framework, which open new policy and regulatory avenues for smart cities and other data donation contexts. We also show how some dimensions of the DDRF may extend to other aspects of the internet that rely on user contributions, such as crowdfunding, blockchain and knowledge bases.

Jasper Verstappen and Gerard Jan Ritsema van Eck:

'U can't touch this: data protection, data ownership, and informational self-determination'

Personal data stores/services (PDS) have been advocated as a socio-technical counterweight to global surveillance capitalist enterprises' expanding dominance. By allowing granular access to third parties, an individual obtains complete control over personal data flows by using a PDS. This paper explores the link between a person and their data from the perspectives of European data protection law and private law against the background of PDSs. By analysing the perspectives that these fields of law take, we aim to explore a more fundamental question about the nature of these legal fields. The underlying aim of this paper is thus to determine if the thinking that has developed in the domain of private law on data ownership, can be used to augment developments in data protection law. Specifically, we anticipate that the considerations underlying data ownership will support the concept of informational self-determination. PDSs are a tool to put personal sovereignty into action. This provides fertile ground for analysing the interplay between two rapidly developing fields of law in the context of an innovative application of technology aimed at protecting the self-determination of data subjects.

Jonas Breuer, Ine van Zeeland and Jo Pierson:

‘Walk the Talk before you run the Risks – Walkshops for Citizen Involvement in Data Protection Impact Assessments'

How do we find a way to involve citizens in assessing the risks of smart city projects? Challenges are numerous: citizens may lack the digital literacy to evaluate technology on paper or the resources to participate in a formal procedure, and smart city decision-makers may be wary of time-consuming public consultations, to name but a few impediments. This paper evaluates the utility of ‘walkshops’ – part city walk, part workshop – as a low-threshold approach to hearing citizens’ perspectives on the ubiquitous processing of personal data in public space. We show that walkshops can potentially be used to seek citizens’ views in the Data Protection Impact Assessments mandated by the EU’s General Data Protection Regulation. Our results from ten walkshops in three Belgian cities show that citizens need to feel informed to trust authorities’ use of personal data, which will require more than meeting minimum transparency requirements. Perceptions of surveillance can be a risk in itself, negatively affecting the acceptance of technology-based interventions. We show how the embodied experience of walking through the ‘smart city’ to gather perspectives from various stakeholders can contribute to a higher quality of risk assessment and to more proportional decision-making on data collection in public space.

Law & Technology

Moderator: Rosamunde van Brakel

Sergio Genovesi and Julia Maria Mönig:

‘Unintended Surveillance as an Impact Factor for a Certification of Ethical AI'

The European Artificial Intelligence Act (AIA) attributes a central role to "standards, conformity assessment [and] certificates" (Chapter 5) for auditing and regulating high-risk AI-systems [1]. Annex III to the AIA lists areas in which the use of AI systems will be considered as “high-risk”. This list reads like an enumeration of concerns from the surveillance studies. In order to contain the risks posed by these systems we propose labeling unwanted surveillance as a negative factor in the framework of an ethical certification of trustworthy AI. Following the definition by Gilliom and Monahan [2], according to which surveillance means “monitoring people in order to regulate or govern their behavior”, we investigate how some AI applications have as an unintended side effect the regulation and discipline of their users’ behaviors through monitoring. If an AI application is not designed for legitimate surveillance purposes, we suggest that triggering surveillance dynamics as a side effect should be a reason to not grant a certificate.

Gabry Vanderveen:

‘Contesting images: visual literacy and learning to question (counter)surveillance images'

Whether images are made by drones, CCTV-cameras, bodycams worn by police officers, or smartphones of citizens: many images are produced, and shared because of surveillance and countersurveillance practices. These images can be used as evidence. They are so-called evidence verité: real-time footage, CCTV-images and photographs. “Reading” these images, interpreting the meaning of these images is not straightforward, though many people think so. Biases, and for example the effects of framing, context and our own prior knowledge affects how we interpret an image. Films and photos as evidence have increased since the Nürnberg Tribunal (1946). Various non-governmental organizations (NGOs) and citizens use countersurveillance to document police conduct and human rights violations in photos and films. This can only serve as evidence in (international) criminal law when they meet certain criteria. NGOs and the OSINT-community try to prevent biases and have guidelines for collecting visual evidence (e.g. the Berkeley Protocol). Because of the increase of visuals in the legal system, several scholars argue for more attention for visual literacy. We study what & how Dutch police learn about the interpretation of (counter)surveillance images and how this can be improved. This paper discusses the research projects and findings so far.

Gerard Jan Ritsema van Eck and Nynke Vellinga

‘Watching you watching the road: Do drivers need to compromise privacy for road safety?’

In a debate style, we will juxtapose the right to life with the right to privacy as we explore novel technological requirements which necessitate that cameras continuously monitor and analyze car drivers. Nynke Vellinga will defend the right to life: Thanks to the smartification of cars, it is now possible to monitor the driver’s alertness and distraction. This new technology has the potential to save lives as sleeping and distracted drivers are major causes of road traffic accidents. With 1.35 million fatalities each year and given the right to life guaranteed by article 2 of the European Convention on Human Rights (ECHR), this technology should be deployed. Gerard Ritsema van Eck will defend the right to privacy: Sealed from the outside world, the interior of an automobile offers drivers a high degree of privacy. Article 8 of the ECHR safeguards this privacy against unwarranted intrusions. The new EU General Safety Regulation violates this right to privacy by requiring driver drowsiness and distraction detection systems. Individuals can not be forced to give up their individual rights for public interest in road safety. In this interactive conversation we will ask participants: where would you draw the line?

Human Rights (1): Asia

Moderator: Ernestina Konadu Duodu

P Arun:

‘Undemocratic Legality”: Communications Surveillance Regime in India’

In January 2021, in the ongoing case of the Delhi High Court challenging India’s communications surveillance regime in Centre for Public Interest Litigation v. Union of India, the Ministry of Home Affairs made an unprecedented argument in their submission. It was argued that the secretary in-charge of Legal Affairs (Law Secretary) applies the ‘judicial mind,’ and performs ‘judicious review’ to the directions given under Rule 419A Indian Telegraph Rules. An uncanny coincidence occurred in October 2019, when a serving district and sessions judge, Anoop Kumar Mendiratta was appointed for this post on a contractual basis. The Home Ministry’s submission along with this appointment raises a doubt, whether this move would democratise while initiating a longstanding call for reforms in the prevailing executive oversight over the executive. This is not an isolated incident, rather in the last two decades, there was a larger trend surrounding India’s communications surveillance regime, which could be described as ‘undemocratic legality.’ This paper will discuss the phenomenon of ‘undemocratic legality.’ How come despite not being even close to the commitments to the fundamental essentials of the rule of law, neither in a narrow nor robust sense, they continue to exist? How with inadequate safeguards and bare minimum rules India’s communications surveillance regime is being extolled as lawful and thus continues to exist as part of Indian democracy?

Amira Paripurna:

‘Access to Justice for Communications Surveillance: Improving Democratic Policing Model and Mass Surveillance Policy'

The two recent reports released by the Southeast Asia Freedom of Expression Network (SafeNet) and Amnesty International found that Indonesia moved closer to digital authoritarianism. The National Police’s move to launch a “virtual police squad,” or cyber patrol. The virtual police cyber has the power, among others, to conduct wiretapping and monitor conversations that occur in WhatsApp groups. It is an effort to eradicate crime and suppress the circulation of hoaxes. However, this effort has sparked widespread fear of excessive state surveillance at a time when cybercrime is on the rise in Indonesia. It is also contrary to the reformation measures taken post the authoritarian regime that the Indonesian National Police promotes and implements democratic policing.
The extraordinary power that allows police, intelligence, and security services to conduct communications surveillance programs, especially (indiscriminate) interception, should meet specific criteria. As proposed by international human rights treaties, this entails that these activities should have a law-standard quality (to be accessible and foreseeable), should have a legitimate aim (to protect national security), and that the interference must be necessary and proportionate. On a state level, the extent to which accountability mechanisms adequately deal with the side-effects of (indiscriminate) communications interception differs. For those concerned, access to justice is a crucial method to remedy an alleged intrusion by the police, intelligence, and security services, in addition to oversight bodies.

There are 3 (three) main research questions in this research 1) what criteria using by the virtual police to conduct communication surveillance and interception; 2) what remedies are available for particular groups? 3) do individuals affected by (indiscriminate) communications interception receive access to justice?

Qazi Mustabeen Noor:

‘Surveillance, security, and strange bedfellows: Analyzing Bangladesh’s turn to digital authoritarianism'

This paper argues that Bangladesh’s turn to authoritarianism has been fueled largely by regulation of information and social media surveillance, for which the country has sided with certain “peculiar” forces that does not otherwise coincide with its liberal democratic image. By purchasing surveillance equipment from Israel, a country that Bangladesh has no diplomatic ties with and by giving legal protection to the right-wing religious organization Hefazat-e-Islam under the Digital Security Act (DSA), Bangladesh is not only surveilling and stifling dissenters, but also building itself a legal shield that gives indemnity to various government actors. The work also sheds light on the newly drafted Data Protection Act of November 2020 as to how it creates a catch-22 situation for any individual or group looking to sue the government on charges of information misuse. The Digital Security Act (DSA) and Bangladesh’s secret surveillance equipment deal with Israel were the immediate effects of the 2018 Road Safety Movement in which thousands of school and university students all over the country participated wholeheartedly. This urged the government to embark on a combing operation to not only surveil what is posted on social media, but also heavily regulate the internet to stifle dissent.

Human Rights (2): Russia

Moderator: Candace King

Rashid Gabdulhakov:

‘Online surveillance and exposure of women, feminists and sexual minorities in Russia’

This article presents the case of Male State online vigilante movement in Russia. The movement’s members are notorious for shaming Russian women for dating ethnic minorities, as well as exposing, doxing, harassing physically attacking feminists and sexual minorities, whom they often publicly referred to as “bio garbage”. Perhaps the loudest acts of the group were reactions to progressive advertisements featuring same-sex couples and ethnic minorities. Male State members exposed the featured actors and shared personal information of company employees on the web, calling for mass retaliation. As a result, some of the targets had to flee Russia and seek refuge abroad. In the context of prevailing homophobic and nationalist narratives in the country (often supported by the ruling elites), Male State vigilantes operated freely for three years, until the group was deemed “extremist” in October 2021. This article scrutinizes citizen-to-citizen surveillance approaches in Russia in the context of gender and sexuality. By juxtaposing the official narratives with those of citizen activists/vigilantes, the author argues that state propagated social norms and gender relations in Russia create fruitful grounds for hate groups to surveil, expose, shame and otherwise punish their targets.

Ola Svenonius:

'Countering disinformation: Surveillance and the politics of psychological defence'

Political events during the 2010's contributed to a securitisation of information in Western security policy, most notably the Russian annexation of Crimea in 2014 and disinformation campaigns directed at electoral processes in several Western countries. The paper analyses policy responses in a set of European countries that have created new institutions to identify and counter disinformation and "hybrid threats". In Sweden, the Agency for Psychological Defence began its operation on January 1, 2022. In France, a similar agency started in 2021. Other countries, such as Denmark, Finland, the Czech Republic, the UK and Germany, have all created institutions or government offices to identify foreign influence, perform countermeasures, and coordinate research on these new types of threats. In addition, the EU and NATO have created centres with similar tasks. However, disinformation is difficult to detect – what is legitimate public debate and what is illegitimate influence by antagonistic state actors? The politics of disinformation and hybrid threats entail a classic dilemma: How will basic rights such as freedom of speech be protected and disinformation countered at the same time? The paper compares institutional arrangements in seven European countries with the aim to study how this dilemma between surveillance and democracy has been negotiated.

Human Rights (3): MENA
Moderator: Elham Fatapour

Anna Lichinitzer and Itay Snir:

'Self-Surveillance as Resistance: CCTV and Tribal Authority in the Bedouin Town of Hura'

In this study we examine the installation of surveillance cameras in the Bedouin town of Hura in the Negev desert in Israel, analyzing the complex interactions between the state and the local inhabitants. Considering the long history of Jewish colonialism in the Negev and the application of a wide array of instruments to oppress the Bedouin population, it might have been expected that the introduction of the new surveillance technology be a state-directed initiative, in which the local population would be either passive or reluctantly cooperative. However, in-depth interviews with Hura inhabitants demonstrated that the municipality and tribal chiefs were active players in deciding on the installation and location of the cameras. We argue that while the cameras placed the inhabitants under a new layer of surveillance, their installation could also be understood as an act of resistance to the ongoing neglect of Bedouin lives and possessions by the state.

Merouan Mekouar, Ozgun Topak and Francesco Cavatorta:

‘Authoritarian practices in the age of digital surveillance in the MENA region’

In response to the recent local and regional uprisings (notably the 2009 Green Movement in Iran, the Arab uprisings of 2011, and the 2013 Gezi Protests in Turkey), the countries of the Middle East and North Africa (MENA) region have refashioned ‘established’ authoritarian practices (such as repressive laws, imprisonment of dissidents and extra-judicial killings) and added new mechanisms of surveillance (such as internet and spyware surveillance) to stifle dissent, neutralize opponents and prevent social mobilization. The presentation will show that MENA regimes are using a mix of historically-established practices and new authoritarian practices in conjunction with one another to form what Topak (2019) calls an “authoritarian assemblage”. Assemblages combine, for instance, police violence against street protesters with surveillance of dissenters on social media. A mix of old and newly-adopted legislation, is also deployed to criminalize offline and online dissent, thus complementing the other elements of the assemblage. A case in point is the brutal murder of Saudi dissident journalist Jamal Khashoggi where spyware surveillance is combined with extra-judicial killing. This presentation will draw on this and other cases from the authors’ forthcoming book “New Authoritarian Practices in the Middle East and North Africa” (Edinburgh University Press, 2022), based on the analysis of old and new authoritarian practices in seventeen MENA countries. Particular attention will be given to the expansion of digital surveillance practices and how they interact with historically-established authoritarian practices.

Youssef Mnaili and Leila Seurat:

‘TAGASUS - Transferring to Arab Government Surveillance Systems. The Case of the United Arab Emirates'

Shoshana Zuboff's Big Other concept captures the paradigm shifts provoked by surveillance capitalism and its seemingly free services. The Big Other brings with it “new possibilities of subjugation... as this innovative institutional logic thrives on unexpected and illegible mechanisms of extraction and control that exile persons from their own behavior.” Our paper disrupts the Big Other’s pervasive illegibility by comparing three examples of global cinema. In the process, we fill in historical blind spots in Zuboff's framework. To underline the Big Other’s new subjugations, our interdisciplinary paper traces the line between what constitutes just and the unjust surveillance within business. Our examples feature both enthused surveillance capitalists as in James Ponsoldt’s adaptation of "The Circle" (2017) as well as confused, even terrified end users in Kiyoshi Kurosawa’s horror film "Pulse" (2001). We then frame the historical roots of such mass surveillance by situating studies on Big Data’s role in the Holocaust against Quentin Tarantino's WWII film "Inglourious Basterds" (2009). Our comparisons illustrate the consequences of the Big Other's emergence: to be reduced to data is to accept the possibility of being deleted. Ultimately, these films give surveillance and information ethics scholars a new language to map out surveillance capitalism’s trap.

Michael Dahan and Mouli Bentman:

‘Seepage and Delegitimization of Surveillance Technologies in Israel (working title)’

In recent decades, the Israeli state has vastly improved its surveillance capabilities, in particular digital surveillance, using these regularly to control and oppress Palestinian society (Dahan, 2013; Zureik, 2020). The current pandemic pushed Israel to implement similar measures and technologies to monitor and surveil Israeli citizens, in an attempt to control the outbreak. Then Defense Minister and current Prime Minister Naftali Bennett went so far as to suggest using the tools in NSO's stockpile to locate and track verified Covid19 infections among individual citizens. On the tail end of this, wide scale surveillance of Palestinian Israelis is close to being implemented in the context of the "war on crime". The use of security services for large-scale surveillance of Israeli citizens reveals several significant issues: 1. The seepage of surveillance technologies from military to civil sphere. 2. The weaknesses and shortcomings of these technologies resulting in a heavy price paid by voiceless populations who stand helpless in the face of false claims by security organizations. 3. The use of technologies, even during a pandemic, leads to a change in the behavior of citizens. In our paper we argue that the increasing surveillance of the population did not have the desired results but rather was ineffective in breaking the chain of contagion, resulting in the loss of public confidence in the system in general, while raising further questions regarding the legitimacy of using such technologies.

Human Rights (4): China

Moderator: Fieke Jansen

Marcella Siqueira Cassiano:

'The Digital "Dom-ino": The Household Register and China's Surveillance Apparatus'

The concepts of off-site construction and piece-assembling have been around for centuries. However, it was not until the French-Swiss architect Le Corbusier created "The Dom-ino House" in the 1910s that prefabrication and modularity became an open-ended concept and an economic process of modulation that is conducive to building flexibility. We draw on the "The Dom-ino House"—a void modular structural skeleton formed by three horizontal slabs, six columns, and a lateral staircase that allows for infinite building variations—to interpret the transformation of China's surveillance apparatus since 1958 and discuss its social and political implications. Chinese surveillance revolves around the Household Registration System or simply hukou, a versatile digital modular structure that counts and classifies Chinese families and their members from numerous perspectives. Working like Le Corbusier's Dom-ino, hukou is conductive to numerous and flexible surveillance practices. Since the late 1950s, hukou has been plugged with several surveillance modules that regulate, among other domains, access to the internet, neighborhood services, policing, geographical mobility, and, since the COVID pandemic, contagion risks. As a "digital domin-no," hukou offers all levels of government in China the ability to develop ad hoc and long term "plug and play" modules that surveil different aspects of life and present and a significant source of knowledge of China's 1.4 billion people, which the Communist Party taps into to ensure its sovereignty.

Hui Fang and Shangwei Wu:

‘"Life and death" on the Chinese internet: Body metaphors and Chinese internet users' experiences of "account bombing"’

Since 2018, narratives about a specific measure of internet censorship have emerged on the Chinese internet; netizens call this "account bombing" (炸号). It refers to the phenomenon that some social media accounts are blocked permanently by internet regulators without the users knowing the reasons for this or receiving any warnings in advance. Unlike the case of "digital suicide" where users actively disconnect themselves from social media (Karppi, 2011), account bombing as a type of internet surveillance can be devastating for users, especially when the social media platform (e.g. WeChat) is significantly intertwined with users' daily lives. Aimed at understanding how Chinese internet users make sense of account bombing experiences and react to internet surveillance, this study examines users' narratives about this practice, especially the metaphors they employ. It contains a critical metaphor analysis (Charteris-Black, 2004) of preexisting online narratives and semi-structured interviews. Preliminary findings suggest that the users often use the metaphors related to the body, such as “ghost”, “reincarnation”, and a person's "will". These body metaphors reveal the irreversibility of account bombing and the uneven power relations on the Chinese internet which are heavily skewed toward regulators. Body metaphors also establish the relevance of this seemly individual, sporadic experience to a broader audience, evoking sympathy both affectively and politically.

Lotus Ruan and Lianrui Jia:

‘Caught in Between: An Analysis of Privacy Issues Surrounding China-based VPNs'

Millions in China use Virtual Private Networks (VPN) services to circumvent the Great Firewall of China, a technical system built to keep politically sensitive websites and undesirable content from appearing on the Chinese Internet. However, as more Chinese increasingly reside outside of China a niche market has sprung up: VPN services that route online traffic back to China to access geo-blocked content and services that are only available to Chinese IP addresses (China Digital Times, 2019; GlobalWebIndex, 2015). In practice, however, VPN services can have security and privacy vulnerabilities that are little known to the public (Ikram et al., 2016). While VPN services may prevent data from being visible to network providers and state authorities, the traffic is accessible to VPN providers themselves who theoretically can conduct surveillance on its users (Cyphers & Gebhart, 2019; Constine, 2019). In this paper we provide the first comprehensive analysis of 11 VPN products that are marketed to provide China-bound VPN services for overseas users. Our research methodology consists of three parts. First, we review these applications’ privacy policy policies and terms of services documents for Android and Apple mobile users on the following dimensions: data collection and storage, data transfer, data use and disclosure. We then apply a research methodology adopted by the Citizen Lab (2019) in which uses Data Access Requests (DARs) to measure how, or whether, these providers respond to these requests in practice. Third, we conduct technical analysis of these applications and capture what data is actually being collected and transmitted. The triangular research components will provide empirical data about the protection of privacy and against surveillance in a highly obscure yet trusted service to bypass surveillance and geo-restrictions.

Ausma Bernot and Sara Davies:

The social sorting of queer activists in China post-Covid: The marginalising effects of automated digital surveillance'

In China, LGBTQ+ activism has existed in a grey space between non-criminalisation in legal terms and fragmented strategies of suppression in reaction to activities of queer communities. The expansion of home-grown social media platforms in the past decade has provided a (relatively) safe haven for LGBTQ+ people to connect. Prior to 2021, digital LGBTQ+ communities, primarily facilitated via the popular social media platforms of WeChat and Weibo, were an important part of queer life in China. In June 2021, mass closures of LQBTQ+ social media accounts disrupted communications of queer communities and individuals that were particularly crucial during Covid-19 lockdowns. Considering the increasing restrictions in the digital space, we posit the question of how LGBTQ+ activists and communities in China have responded to the changing conditions of digital surveillance. In this exploratory study that centers the voices of LGBTQ+ activists and communities in China, we analyse the effects and responses to increased surveillance in digital spaces during and after Covid-19. David Lyon's theory of social sorting is the conceptual framework that thematically organises the findings. Our preliminary findings suggest that the LGBTQ+ communities in China have been negatively affected by the increased digital surveillance.

Human Rights (5): Europe & Global South

Moderatore: Francisco Klauser

Bram Visser and Rosamunde van Brakel:

'Legitimate police use of digital surveillance? Addressing concerns about the Belgian governance framework'

The increasing reliance on digital surveillance infrastructures by police agencies has attracted the necessary headwind over concerns for fundamental rights violations and socio-technical harms. The EU Law Enforcement Directive (LED) provides a legislative framework for member states to regulate data protection for police agencies' crime fighting activities, including the possibility to set up a completely independent supervisory authority. As one of the few to do so, Belgium established the Supervisory Body for Police Information (COC). The aim of this paper is to address legitimacy concerns with the way police use of digital surveillance is governed in Belgium. The hypothesis underlying this research is that the governance framework for police use of digital surveillance in Belgium is insufficient to cope with the risks of regulatory and statutory capture identified in the literature. We argue that a recent decision by the COC exposes statutory capture and this is at least partly due to the faulty transposition of the LED into Belgian law (police law and camera law). Additionally, certain elements in the body's constellation and institutional arrangement may point to other forms of regulatory capture. In the paper we highlight the main challenges and suggest improvements and best practices.

Bárbara da Rosa Lazarotto:

'The use of private databases by States for surveillance purposes and its implications to individuals' fundamental rights.

The advancements of technology for the last decades transformed the lives of citizens into a reality that was only imaginable in a sci-fi movie. Streets are full of private cameras, almost every individual has a social media account where they post their most intimate details, several types of gadgets have numerous tasks. All of these examples generate a huge amount of data that is stored in private databases owned by private companies. Before the creation of the "technological world", States were the ones that held the majority of individuals data, such as birth certificates, death certificates and so on. However, now this logic has been reversed, now it is safe to say that private companies have the largest and most private amount of individual data. Thus, this paper aims to discuss the use of private databases by States for surveillance, such as facial recognition technologies and how this use impacts the fundamental rights of individuals.

Joan Manuel Lopez Solano:

'Experimenting with poverty: social registries and the violence of automated systems in Colombia'

The Sistema de Identificación de Posibles Beneficiarios de Programas Sociales (SISBEN) is the main instrument to classify the Colombian population in terms of poverty. This system is used to select the beneficiaries for at least 19 social programs. In 2016, the government made two changes in the system to respond to a growing number of people eligible for social aid. First, a secret algorithm tries to predict the "capacity of income generation" of each household, and second, they will crosscheck the data provided by the beneficiaries with 34 public and private databases including credit reporting agencies like Experian. The government in collaboration with international organizations constructed a discourse in which AI and Big Data would reach "the real poor". The idea behind the new Sisben is to assess the social conditions of citizens and determine beneficiaries of social programs using the data that they give in the interaction with the public and private actors to update the information. The new Sisben exposes a new arrangement of social protection programs in which, rather than having a complex and massive interview process, access to social rights would be granted using secret and automated mechanisms that predict the behavior of vulnerable citizens. The paper analyzes the narrative behind these changes, the risks of perpetuating the violence of living in poverty through data technologies, and the limitations of data protection frameworks to analyze the implementation of data systems in the South

Mehak Sawhney:

'Pegasus and Espionage in India'

This presentation seeks to reflect on the use of the Pegasus spyware in the Indian context since 2019. A discussion on Pegasus appeared for the first time in India after the 2019 general elections when the mobile phones of multiple journalists, politicians and activists were hacked. Pegasus, which has been called a weapons-grade cybertechnology, was developed by an Israeli technological firm called NSO, which claims that the software is sold only to governments for tracking terrorists and criminals. The most concerning feature of Pegasus is its zero-click feature which requires no user interaction for its activation. This presentation will trace the parallel emergences of the phone as a computational medium as well as the use of spyware to discuss the entanglements between espionage, state surveillance, and political dissent in India. My presentation will speak to three main themes of the conference: digitally mediated surveillance, sensing beyond seeing, and law, justice, and surveillance.

Privacy Law

Moderator: Lucas Melgaço

Bryce Newell:

'Reclaiming Privacy: Surveillance, Informational Power, and the Limits of Data Privacy Law'

Recently, the United States has seen a renewed push to adopt more comprehensive data privacy laws. While some of this trending shift toward "protecting" privacy has no doubt been motivated by the seemingly endless (re)occurrence of privacy catastrophes at the hands of big tech companies, we have also seen how corporate interest in having more uniform privacy law across the country has spurred corporate engagement and lobbying in this process. In this paper, I examine the rise of these so-called "comprehensive" data privacy laws within the US (e.g., in California, Virginia, and Colorado) and argue that these laws facilitate too much corporate surveillance, provide too much access to personal data to law enforcement agencies, and do not go far enough in protecting individual privacy rights. I draw from neorepublican political theories of freedom and privacy to show how these new "comprehensive" data privacy laws fail in many ways to restrict the arbitrary use of informational power by corporate and state actors -- allowing potential domination. Finally, I suggest ways in which these privacy laws could be revised to more adequately account for and counter domination and provide individuals and communities with greater "antipower" in the fight to reclaim their privacy.

Joe Purshouse:

'Police Surveillance in the United Kingdom Courts - Taming Strasbourg?'

The UK has witnessed a near unfettered rise in police surveillance over the course of the last three decades. Ironically, this rise has occurred in conjunction with an ongoing 'human rights revolution', whereby human rights law is said to have transformed the law of criminal procedure and the conduct of police evidence gathering. This correlation is unexpected. It raises questions concerning both the value of human rights law as a bulwark against authoritarian police surveillance; and the extent to which have UK judges lived up to their role as the 'guardians of human rights' responsible for tempering the use by police of surveillance technologies to ensure compatibility with the European Convention on Human Rights (ECHR). Through close examination of the reasoning of judges in domestic police surveillance cases, this paper examines how the senior domestic courts have produced and maintained the ‘legality’ of increasingly intrusive modes of police surveillance by unduly narrowing the protection afforded that could be afforded by the ECHR to those targeted by police surveillance. Thus, the courts have extended the power of the police to subject the population to surveillance through, rather than in spite of, their ostensible embrace of human rights principles, laws and discourse.

Michaela Padden:

‘The transformation of mass surveillance in data protection discourse: A brief genealogy'

This paper presents the results of a genealogy of data protection discourse from the 1950s to the present, with a focus on “problem representations” of mass surveillance (Bacchi 2012: Bacchi and Goodwin 2016). The paper traces the ways in which both potential ‘harms’ and ‘benefits’ of mass surveillance practices have been articulated in both the ‘free flow’ and ‘rights based’ discourses of data protection policy. Particular attention is paid to the emergence of these two discourses in the 1970s, in the discussions leading up to the publication of the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data by the Organisation for Economic Co-operation and Development (OECD) in 1980. These Guidelines formalised a set of ‘data protection principles’ which remain a key feature of EU data protection regulation. The study follows the OECD’s representations of mass surveillance as a policy ‘problem’ from this period to the present time, highlighting key moments in data protection discourse which help to show how mass surveillance practices, once broadly considered verboten, are now commonplace. The key finding of the paper is that the increasing utility of surveillance techniques to generate profit has precipitated a shift from generally bipartisan agreement over the incompatibility of mass surveillance with democracy, to an increasing acceptance of mass surveillance practices, re-branded as tools to promote efficiency, transparency, customisation and economic growth.

PANEL: Privacy Studies, Surveillance Law

Panelists:

Bert-Jaap Koops

Daniel Susser

Maša Galič

Lisa Austin

Scott Skinner-Thompson/Bryce Newell (Chairs)

Surveillance studies and privacy law have synergies. With roots in the social sciences, surveillance studies scholars do critical work documenting (historically, quantitatively, or qualitatively) how surveillance systems negatively impact people in their day-to-day lives. With their doctrinal pedigree, privacy law scholars are often focused on law and policy solutions to violations of personal privacy. Both disciplines draw from philosophical traditions to theorize how surveillance systems contribute to social control and subjugation. And while there are, of course, examples of privacy law and surveillance studies scholars drawing from each other and collaborating with each other, the potential synergies of these two related disciplines seem underutilized in their shared goals of combatting surveillance abuses and enhancing the lived experiences of the marginalized communities who are often disproportionately impacted by surveillance systems and policies. In this Panel, while panelists are still finalizing their ideas for independent contributions, scholars from both fields will discuss how their discipline's scholarship might benefit from additional cross-pollination (and vice versa). In particular, panelists will reflect on the following questions. How do these fields' disciplinary orientations constrain inquiry or intervention? To what extent does privacy law fixate too heavily on extraordinary or outlier cases, without attention to on-the-ground impacts of surveillance networks? Conversely, would surveillance studies as a discipline achieve greater impact if it gave more attention to pragmatic solutions? What are the specific theoretical insights that ought to receive greater attention in each discipline? The panel will be organized as a moderated discussion Professor Bryce Newell (University of Oregon) and/or Professor Scott Skinner-Thompson (University of Colorado Law School). The panel is being hosted by the Dialogue section of the S&S journal and will provide a forum for discussion about work to come out in a latter issue of the journal.

STREAM 4: SECURITY & POLICING

Borders & Migration (1)

Moderator: Julia Maria Mönig

Hakan Ünay:

'Border Measures as New Tools of States' Surveillance: An Analysis of Turkey's Measures Against Immigration at the Syrian and Iranian Borders'

This study aims to analyze the border measures taken by states against immigration through Turkey. Borders have been places of sovereignty, power, and security of states for many years. While the factors that the states see as a threat have transformed over the years, the mission of the borders, especially in the 21st century, has focused on surveillance and prevention. The problems experienced in different geographies of the world and the fact that immigration and immigrants have become a global agenda have started the trend of taking precautions at the borders of states. Turkey is one of the states that has kept up with this trend with the measures it has taken against mass migration on the borders of Syria and Iran in the last 5 years. Being on the migration route of millions of immigrants from different nationalities, especially Syrian and Afghan immigrants, Turkey has increased its border measures in recent years. Turkey, which has built a wall on the borders of both countries, has further increased its precautions with the surveillance technologies integrated into the wall on the borderline.

Jan Waszewski :

'"Digital walls" from the perspective of Belarus–European Union border crisis of 2021'

The European Union's member states neighbouring the Belarus faced a migrant crisis in 2021. One of the solutions to the problem of illegal border crossing has become the construction of border walls. The concept of digital wall was also part of the answer. It hasn't been the thirst time that computers, artificial intelligence, automated biometric identification systems, big data analytics and other surveillance tools has been presented as the most sophisticated, modern, and best solution to some problem. The paper proposes that the surveillance studies give the insights into "the 5W" of building the digital walls. Who decides, and who benefits, and who will be subject of surveillance? What processes are taking place? When and if something will in fact probably happen? Where digital walls will be built, and will this concept spread: will it enter (i.e.) the social media and other communication channels? And finally, the most important question: why digital walls are seen as the solution?

Lauren Elrick:

'The More You Know': Generalising the Surveillance of Migrants through the EU's Border Security Ecosystem'

Beginning with the Schengen Information System in the 1990s, the EU has developed an ecosystem for information exchange within the border security field. Through a series of large-scale IT databases (SIS, VIS, Eurodac, EES, ETIAS, ECRIS-TCN), and most recently, the introduction of interoperability, the EU has sought to maximise their ability to collect and exchange the personal information of third country nationals (TCNs) between member states. Many of these databases, while originally conceptualised as migration management tools, have subsequently come to be recognised as beneficial to achieving security-related goals. Consequently, they highlight a growing trend through which the mobility of TCNs has come to be securitised, enabling every increasing forms of surveillance to be legitimised. Through analysing relevant legislation and EU policy documents, this article seeks to show how the EU has sought to develop new databases in order to close information gaps and enact a system through which the movements of TCNs can be monitored and assessed, potentially even before they enter the European territory. In doing so, migrants increasingly come to be seen as a suspicious group, requiring enhanced surveillance, an action which has important implications for the protection of human rights, such as privacy and non-discrimination.

Borders & Migration (2)
Moderator: Azadeh Akbari

Veronika Nagy:

'Late Modern Surveillance in Europe: Self-censorship in a Digital Asylum'

In the last decennia, as a result of neoliberal policies, affective aspects and perception-based policies dominate global control and surveillance measures. Following the critical surveillance studies tradition of qualitative data analyses, this research explores how unattractive mobile

groups, - considered as suspects of terrorism and organised crime - are increasingly subjected to social sorting through mobile surveillance within and even outside the virtual walls of Fortress Europe. Due to tech literacy and surveillance awareness, monitoring practices are also shifting technocratic policing practices, which leads to changes in interactions between newcomers and host authorities. These modifications can be traced by mobile ethnographic studies that are able to interpret the situational understanding of self-censorship in daily practices of migrants. Using multi/sited analysis of refugee surveillance, this research addresses policing incentives in the EU and how surveillance subjects as forced migrants from conflict countries use coping strategies by digital devices to prevent legal expulsion. The central research question is: How does the digital turn in surveillance change the way we approach organized crime issues in the migration domain?
The objective: To better understand the impact of heavy surveillance on stigmatized mobile groups
The method: Multi/sited analysis of refugee surveillance data
The results: Preliminary; self-censorship is an attempt at resisting expulsion

Ozgun Topak:

‘Refugee Vetting Surveillance: the case of Canada and Syrian Refugees'

This presentation is about the surveillance practices deployed in the refugee vetting process. It will examine the case of Syrian refugees who were resettled to Canada, or rejected from resettlement based on security and truthfulness grounds. Refugee vetting surveillance includes detailed interviews, biometrics, social media surveillance, phone surveillance, and more recently algorithmic surveillance. It also includes data-sharing among Canadian and the US security agencies, and international database checks. The vetting officers use these surveillance practices to assess the credibility of the applicants and the level of security risk they pose. This paper will draw on official documents, legal cases, and interviews to analyze Canada’s refugee vetting surveillance and its consequences for the refugees/applicants who experienced the process. As a humanitarian form of surveillance, refugee vetting surveillance contributes to the normalization of invasive and extreme surveillance (or ‘extreme vetting’), deepens surveillance hierarchies and power asymmetries, and results in discrimination.

Ana Valdivia and Claudia Aradau:

‘Methods, systems and devices: Patenting and the datafication of EU’s borders'

Borders and migration management have become important sites for data processing and technological surveillance and innovation. Yet, little is known about the specific details of algorithmic systems that private companies develop and implement at the borders. In this paper, we propose to investigate patents, which have been a neglected empirical site for research on borders and technology, to better understand how algorithmic systems are deployed to control migration flows. We focus on patents of companies that have been awarded contracts by the European Union Agency for Large-Scale Information Systems (eu-LISA) to develop new databases that extend biometric data processing and interoperability. Patents are publicly available and structured documents that are important in three respects. Firstly, patents afford in-depth insights into the specific technologies that a private actor sells and implements beyond marketing and advertising materials. Secondly, by using digital methods, we can develop a systematic analysis of problematizations and sociotechnical imaginaries of these innovations. Thirdly, our transdisciplinary research allows us to disentangle the specificities of technologies to investigate their ethico-political implications. This methodology helps shed light on the political assumptions and ethical implications of the methods, systems and devices patented by private companies developing EU's datafied borders.

Borders & Migration (3)

Moderator: Amanda Glasbeek

Martina Tazzioli and Ana Valdivia:

'The borders of biometric surveillance: questioning the hype of facial recognition through the lens of migration'

This presentation argues that the border constitutes a critical vantage point from which to investigate modes of racialised surveillance which are enforced through biometric technology. Building on Simone Browne's statement according to which the border is a site where a critical biometric consciousness can be developed, we illustrate that biometrics at the border is used by multiplying racialised modes of surveillance. In this sense, a close scrutiny of the way in which migrants are differentially targeted and categorised through biometric systems allows us to problematize the image of the subject who is implicitly at stake in critical analyses of technology as a white citizens. The border is in fact a site where a homogenous gaze on technology appears inadequate for capturing the hierarchies of rights protection. What do we see if we look at biometric surveillance technology from the standpoint of those who are classified as "migrants"? Drawing on this question, in the second part we deal with campaigns and criticisms raised against facial recognition: while this biometric technology is bringing a vast attention in critical technology debates, seeing like a migrant allows us to realise that there are other types of biometrics that are also jeopardising fundamental rights.

Gokce Onal:

'Sensory reaches of border policing: a media materialist account of remote surveillance'

Border enforcement technologies are increasingly deployed on the security models of total situational and operational awareness. Research on border policing has been rendering visible the ethical, political, and juridical repercussions of this expanding hyper-surveillance matrix. Yet, a physical breakdown of the prevalent monitoring and targeting tactics are yet to be realized. This paper presents a media-materialist reading of the (multi)sensory border infrastructures that are gradually culminating in the concept of smart —or virtual— walls. It sets out on the aerial, earthbound and subterranean reach of surveying machines that do not precisely "see" but rather breech, tap and reconfigure the radiated energies of border-crossing bodies, their belongings and their spaces of transit. In the process, subjects and ecologies become remotely-extracted values of electron densities, surface patterns, spectral and olfactory signatures, and acoustic reflections. Following Campbell's security milieus (2019), this paper argues that sensing machines at borders —while operating through extremely narrow domains of waves, particles, electric currents and digits— engender new spatialities of recognition, targeting, filtering and elimination of the bodies in transit.

Azadeh Akbari:

'The Code-Body at the EU's Digital Corporeal Borders'

The European Union has gradually intensified its gathering of biometric data of immigrants, refugees, and asylum seekers, and increasingly makes the resulted data banks available for several immigration-related and Police institutions throughout Europe. Where legal, political, and humanitarian efforts fail, asylum seekers, try to distort their bodies as the source of undesirable biometric data. With methods such as burning fingertips or claiming to be an unaccompanied minor, they attempt to escape the algorithm and defy the problematic Dublin Convention. Consequently, the EU uses technologies such as retinal scans or DNA tests to overcome such attempts. The body is marked with borders and carries the tension of identification: every gesture, breathing rhythm, stammering, and sweating could contribute to constructing the wrong "data double" (Haggerty & Ericson: 2016). This paper scrutinises border control's intensification through bodily practices and the dynamism of bodily resistance against such measures. The research addresses the historical interrelations between surveillance, identification, belonging, and citizenship (Lyon 2010) and highlights the data-based exclusion of unwelcome asylum seekers by forcing their bodies to reveal their deception. The extreme datafication of bodies and the countersurveillance struggle both coerce the material body to disappear so that an agreeable code-body can rise.

Conflict

Moderator: Nils Zurawski

John MacWillie:

'Lethal Surveillance and the Limits of Cognitive Autonomy'

Surveillance used to be just about watching. But with the technical integration of multi-domain sensors, collaborative communications, aggregation of big data, algorithmic reasoning, distributed computing, an array of mobility platforms, and the projection of kinetic force, surveillance is increasingly being transformed into a much more significant platform for responding to conflict. Surveillance is becoming a key component of autonomous killing machines. The key feature in dispute is what kind and how much autonomy these platforms should acquire. While much of the debate about autonomy has been about moral autonomy, this presentation focuses on a more limited set of questions around cognitive autonomy in which one of the primary objectives is to maximize both self-direction (independence from human control) and self-sufficiency (ability to resolve high degrees of uncertainty), while successfully achieving outcomes within desired parameters. To the extent that lethal autonomous platforms can fulfill mission objectives without incurring collateral damage, they offer substantial competitive advantages in conflicts (e.g., intimate access to difficult or denied spaces, a speed of response faster than human beings alone can provide, low risk to one's own forces, etc.). I argue that if the challenges of cognitive autonomy are resolved, a multinational arms race will obviate the immediacy of many of the moral and political objections to these kinds of technology, in which surveillance becomes sur-la-vie.

Joshua Reeves:

'Military Surveillance and Media Escalation'

This paper examines the conceptual relationship between military surveillance and what Friedrich Kittler calls "media escalation"—the tendency of media technology to advance according to a unique logic that exceeds human plans and expectations. As Kittler and others have argued, this escalation is most evident in military C4I (command, control, communications, computers, and intelligence). Accordingly, this paper analyzes the impact that media escalation has on procedures and technologies of military surveillance, especially as this escalation fuels an increasingly common military goal: the elimination of decision-making human personnel in the command chain, and hence the processual automation of surveillance, enemy recognition, and enemy engagement (drone strikes, e.g.). Because it is taken for granted that humans lack the memory, speed, and endurance of computers and related new media technologies—and because involving humans in command requires elaborate and expensive methods of sending data from the battlefield to decision-makers—human soldiers are less trusted to make even major decisions based on this surveillance data. This line of inquiry coincides with surveillance theory, more generally, because it explores the extent to which the principle of technological/media escalation, rather than human decision, guides surveillance policy and practice.

Emma Hulik:

'Urbicide in the War on Terror in Xinjiang'

Over the last half-century, urban spaces have become inextricably intertwined in modern warfare. Advancement in technologies of warfare and expansion of the sites of warfare have sparked a debate over the classification of new observed forms of political violence. One such debate resides within urban studies, specifically concerning the destruction of the urban space. As warfare has evolved and changed over time, scholars have confronted three central questions related to urban destruction: 1) what is defined as the urban space? 2. what is defined as destruction? 3) what effects are achieved as a result of this particular kind of destruction? Literature on urban destruction reaches far into global pockets of both inter-state and intra-state conflict as well as peacetime modernization of the city, yet no prominent theories have tackled the use of sophisticated, covert 21st-century surveillance technology in the controversial global war on terror. I push for a new conceptualization of urban destruction as a phenomenon of distinct political violence where the built environment is destroyed not through physical de-struction of buildings but rather through the con-struction of a state surveillance apparatus, combining more modern theories of urban destruction as an assault on the urban social fabric (relationships within communities) with critical theories of surveillance and counterinsurgency. I argue that new, highly technological surveillance as a tool of counterinsurgency in the global war on terror constitutes a new form of destruction of the urban space through a case study of China's targeted surveillance of the Muslim-minority population in Xinjiang (also known as East Turkestan). I make my case first through the weaving of an interdisciplinary theoretical framework situated between critical urban, surveillance, and human rights studies, then through a mapping of the evolution of war from post-Cold War era to post-9/11 counterinsurgency warfare, and finally apply the theory to an analysis of leaked official policy documents detailing China's war on terror and firsthand accounts from those living within the total surveillance society in Xinjiang. This research will provide a new framework for understanding surveillance as a tool of warfare against social relations and the possibilities of heterogeneity in the ever-changing global war on terror, with the implications of understanding how the global war on terror violates even the inner-most parts of what makes us human.

Counter-Terrorism (1)

Moderator: A. Haziz-Ginsberg

Jeffrey Monaghan and Fahad Ahmad:

'Socializing the high policing métier: Exploring counterterrorism trainings for frontline workers'

Our article examines counterterrorism trainings for frontline workers as a site of socialization to the high policing métier. Here we build on the notion of the police métier as a term that encapsulates the interactive identities and practices that produce the police world. We twin the police métier with recent scholarship on pluralized policing and surveillance to illustrate how a desire to expand surveillance to plural actors requires a socialization process that recirculates key characteristics, identities, and assumptive worldviews that shape the typically reclusive domains of high policing. Through an ethnographic account of a three day counter-terrorism training workshop for an array of frontline workers, our article analyzes what we consider three key features of socialization within the high policing métier: 1) rationalities of preemption and expanding domains of surveillance; 2) the recirculation of the "war on terror's" racialized fixation on Muslims and Islam; and 3) sharing fraternal moments through the dehumanization of "outsiders."

Itoiz Rodrigo Jusue:

'Mass-surveillance and cultures of suspicion: The promotion of "counter-terrorism citizens" in the United Kingdom'

The growing call for public participation in counter-terrorism in Britain is reflected by the number of recent campaigns directed towards different sectors of the population and, increasingly, towards "ordinary" citizens. This paper examines the promotion of the "CT citizen" as a distinctive political agent and social identity embedded in the participation of mass surveillance and the normalisation of pre-emptive security logics. Based on a critical discourse analysis of the most recent official counter-terrorism and counter-radicalisation websites and e-learning materials (Let's Talk About It, Educate Against Hate, Action Counters Terrorism, and the Prevent duty), I show how citizens are being inscribed as counter-terrorism officials through discourses of responsibility, care, awareness, empowerment, and action. My paper explores the role of British counter-terrorism in the production of new models of citizenship based on a generalised culture of suspicion and in the participation in security duties previously reserved to the authorities. The discussion highlights ultimately that the securitisation of everyday life and the inscription of individuals in "national security" results in the depoliticisation of both the civil society and political violence.

Keith Spiller:

'Counterterrorism performances: impacts of the Prevent Duty in UK Higher Education Institutions'

The UK's Counter-Terrorism measure the Prevent Strategy mandates that public authorities must work to prevent people from being drawn into terrorism. In this paper we review how UK HEIs (Higher Education Institutions) have responded to this new duty by examining the public facing webpages and Prevent policy documentation presented by 158 UK HEIs. In doing this we draw upon de Certeau's notions of the everyday to highlight how such initiatives are presented publicly to viewing audiences, and how messages seep into and deepen surveillance measures within UK Higher Education. In reviewing the performative element of Prevent, specifically how information is displayed, we find that the majority of UK HEIs have approached their new roles through the prism of 'compliance' and/or 'safeguarding'. The paper argues presentations of safeguarding, reassurance and reluctance offer a telling insight into how the Duty has been adopted in HEI everyday practice and the problematic nature of it.

Counter-Terrorism (2)

Moderator: Jorge Pereira Campos

Peter DeBartolo:

'"Ancestries of Interest" and "Countries of Concern": The Reimagining and Remapping of New York City's Ethnic Communities through Post-9/11 NYPD Surveillance'

In response to 9/11, the New York City Police Department (NYPD) launched and maintained expansive demographic surveillance operations targeting neighborhoods and locations throughout the New York City metropolitan area that it associated with designated "ancestries of interest" (Apuzzo & Goldman 2013) and "countries of concern" (Galati 2012). This paper analyzes how particular social and discursive processes enabled the NYPD Demographics Unit to serve a key function in contributing to the production of new, racialized geographical and cartographic knowledge about the City's urban, ethnic communities. It also interrogates the role played by Orientalism and imaginative geography (Said 1978, Gregory 2004, Gregory & Pred 2007) in the development and circulation of such police knowledge (della Porta 1998, Noakes 2006). This research draws on critical human geography and the sociology of race/ethnicity. It contributes to existent scholarship analyzing geographies of surveillance and counter-terrorism in the post-9/11 era (Graham 2004, Graham 2011, Gregory 2004, Gregory & Pred 2007, Klauser 2017) and advances sociological literature addressing racialized surveillance and the War on Terror (Cainkar 2011, Jamal & Naber 2008, Selod 2018). As a qualitative study, this project employs archival research methods (Roche 2021) as well as techniques of Foucauldian discourse analysis (Rose 2016, Waitt 2021).

Lore Janssens:

'An anthropological perspective on the development of the security state in Belgium and its racial-religious contours'

This paper aims to unpack the concept of the security state (Borneman & Masco, 2015; Grewal, 2017) in regard of the Belgian context. To do so, it builds upon ongoing fieldwork in Brussels, as well as 25 interviews that have been conducted throughout Belgium with police and security services and prevention and social workers. Since the start Muslims were at heart of the Belgian anti-terrorism approach, yet it is the period between 2011 and 2017 that was crucial for the development of the Belgian security state. In this period Belgians left for Syria and were implicated in terrorist attacks. This period is characterized by a sense of panic and urgency that, in turn, led to adoption of a big filter: a myriad of old and new surveillance strategies and practices on the Muslim community. The latter had no predecessor in Belgium. Such big filter was only possible due to construction of Muslims as a suspect community. More importantly, these strategies and practices were gradually refined and consolidated into laws and infrastructures of surveillance. Therefore, this period can, alternatively, be characterized as one of experimentation, laying the groundwork onto which the security state was consolidated. This consolidation was legitimized because strategies and practices operated in a legal vacuum and were sometimes improvised. Ultimately, this points to the racial-secular contours that made such a period of experimentation and consolidation possible and thus undergirds the development of the security state in Belgium.

Ayla Zehtab-Jadid:

'Surveillance as care: examining the process of problematization of hate crimes and surveillance in the Canadian government'

The attacks of 9/11 caused a massive shift in surveillance worldwide, and while transformations toward domination and control are well documented, an underinvestigated aspect of this shift is that of the deployment of "surveillance as care." In Canada, the rise in hate crimes towards religious minorities post-9/11 was significant, and as a result, the government invested in new technological solutions to keep these populations and their places of worship safe. Drawing on internal government documents obtained through Access to Information legislation, this paper demonstrates how post-911 hate crimes are problematized as a failure of the securitization of places of worship, as well as how it is that the government of Canada turns to surveillance technologies and discourse of surveillance as care as the solution to this social problem. Specifically, this paper traces the actions and funding distributed through the government of Canada's Security Infrastructure Program (SIP), and the enactment of a discourse of surveillance as care towards religious minorities and the protection of social spaces of worship.

A Haziz-Ginsberg:

‘State on the Line: Empire, Race, and the Coloniality of Lateral Surveillance'

This paper explores the resonances between two distinct deployments of lateral surveillance in the United Kingdom— the Confidential Telephone, which was a key surveillance initiative established by the British in Northern Ireland from 1972 until the mid-1990s, and Transport for London’s (TfL) ongoing “See it, Say it, Sorted” campaign, which was introduced in 2016. Using materials produced by the British Northern Ireland Office in support of the former and TfL and the police in support of the latter, I examine how the deployment of the spectre of terrorism towards securitised ends is not a product of the post-9/11 or post-7/7 period, but is instead part of a broader colonial history of counterinsurgency practices organised around the figure of the terrorist and the citizen-caller. The production of aberration in the name of public safety works to legitimise the state and de-legitimise objects and bodies “out of place” simultaneously. I argue that both campaigns work to forge a constitutive affiliation between the watchful citizen who reports their suspicions and the benevolent, responsive state, and that the affective work these security initiatives do is not incidental, but rather a way of extending existing regimes of racialised surveillance forged through the enactment of British empire domestically and abroad.

Intelligence & National Security
Moderator: Alana Saulnier

Felix Richter, Thorsten Wetzling and Sarah Naima Roller:

‘Civic intelligence oversight: An empirical analysis of practitioners' perspectives in France, Germany and the UK'

In recent years, a multitude of revelations have come to light showing the vulnerability of civil society actors to surveillance by intelligence agencies. New technologies, often combined with overburdened state oversight bodies, have opened up spaces where control is fragmented and at times insufficient. This has contributed to the continued growth of an under-researched form of citizen scrutiny: civic intelligence oversight. Based on workshops with stakeholders and a review of the pertinent literature, we developed online surveys for journalists and for professionals from civil society organisations to better understand the limits and potential of civic intelligence oversight. This paper presents the results of these surveys, shedding light on the structural conditions at work, their resources, their perceived impact, their strategic choices and their attitudes towards surveillance by intelligence agencies as well as their views on state mandated oversight bodies. For both groups, we surveyed practitioners from the UK, France and Germany. The findings reveal a profound dissatisfaction across each sector in all three countries with the existing legal and technological safeguards against undue surveillance, with a majority expressing the need for fundamental reorganisation and reform of the oversight sector. Technical protective measures against surveillance are perceived as effective to some degree, although most respondents believe that a sophisticated attacker can compromise their communications and data. Yet, the respondents’ attitudes towards intelligence agencies were notably different across countries. While French and German respondents predominantly distrust the intelligence agencies in their respective countries, their British counterparts sympathised more strongly with their agencies and expressed less fear of being monitored.

Felix Treguer:

'Is State Surveillance Oversight a Trap? U.S. Intelligence, Computer Surveillance and Their Radical Critiques in the 1960s-1970s

This communication draws on ongoing socio-historical research on computerized state surveillance by intelligence agencies in the United States in the 1960s and 1970s. Using various archival sources including declassified memos from the CIA and other intelligence agencies, it proceeds in three steps to identify a now traditional script in the unfolding and management of intelligence surveillance scandals. First, it shows how actors in and around intelligence worked to promote real-life applications of computers in the context of state surveillance and used these new technologies to expand domestic political espionage against the New Left. Second, it turns to a series of surveillance scandals unleashed over that period, unpacking the desectorization of surveillance and intelligence critique and showing how the transgressions of revealing secret knowledge about the abuse of intelligence while articulating a radical view on democracy and the political dangers of computers became valued stances across various coalesced sectors (in the media, activism, in academia, in the legal and political fields). Third, the paper shows how these scandals led to policy changes, which eventually had a depoliticizing effect on the opposition to state surveillance and disqualified the more radical enactments of state surveillance oversight.

Simon Willmetts:

'Cyber Surveillance, Artificial Intelligence, and the USSID-18 Defence'

In the wake of the Edward Snowden revelations it became clear that different operative definitions of surveillance were animating each side of the ensuing debate. Whilst privacy activists defined surveillance as the acquisition of data, even in unprocessed form, defenders of the intelligence community maintained that it was only once certain data was selected for analysis that surveillance took place. This definition of surveillance was set out in the National Security Agency's internal USSID-18 manual, which provided internal guidelines for the acquisition of data on US citizens. Since the Snowden revelations, however, the US intelligence community has increasingly relied upon artificially intelligent automated surveillance systems, for example the National Reconnaissance Office's (NRO) Sentient research and development program, which in the NRO's own words seeks to "revolutionize" the traditionally sequential intelligence cycle, eroding the boundaries between intelligence collection, analysis and dissemination. When the collection and analysis of data begins to occur almost simultaneously, the NSA's definition of surveillance as only taking place during the "analysis" phase of the intelligence cycle becomes less credible. This paper will explore the impact of artificial intelligence upon the intelligence cycle, and the implications of this for our definitions of surveillance.

Policing & Cameras

Moderator: Joe Purshouse

Diana Miranda, William Webster and Charles Leleux:

‘Governing police-public encounters mediated by the use of Body-Worn Cameras'

Body-Worn Cameras (BWCs) are often depicted as a technological solution to enhance transparent and accountable interactions between police and citizens, with police forces increasingly adopting this technology to capture their interactions with the public. This paper assesses the impacts and consequences of this technologically mediated interaction, and the differentiated governance mechanisms that are emerging around the use of this technology. The paper will provide a brief review of what is known about BWCs, with a focus on mechanisms for oversight and scrutiny in a British policing context. Based on a literature review and set of interviews with BWCs experts, it will also consider the management and use of these cameras in different policing scenarios (examples include armed policing, traffic accidents, stop and search, protests, investigation and domestic abuse). This typology of use highlights different deployment practices and different experiences of use, and importantly the emergence of differentiated governance and scrutiny mechanisms. The paper also considers future challenges for governance arising from the integration of BWC with other emerging technologies and surveillance tools (such as facial recognition and live streaming).

Alana Saulnier and Amanda Courture-Carron:

‘Crafting victim-sensitive BWC policy: Sexual assault and domestic violence survivors’ perspectives on BWCs'

Body-worn cameras (BWCs) are becoming routine in policing globally. BWCs represent a technological shift in the administration of law enforcement. This shift is widely heralded as one that will improve policing. Evidence regarding the effects of BWCs, however, is just now accumulating, with many topics remaining under-researched. The ways in which victims are impacted by police adoption of BWCs is particularly neglected. While interest in the impact of BWCs on victims exists in research (e.g., community members have been asked if they think BWCs will impact victims), only two studies have empirically examined actual crime victims’ perspectives (Goodall, 2007; Toronto Police Service, 2016). These studies, however, do not explicitly consider the perspectives of particularly “vulnerable victims;” – survivors of sexual assault and/or domestic violence, who may be uniquely impacted by police use of BWCs (Adams & Mastracci, 2017). We present data from 33 in-depth semi-structured interviews with vulnerable victims, providing rich insight into the concerns and hopes participants have for police use of BWCs. Drawing on these insights as well as participants’ specific suggestions regarding how BWCs should be used by police, we present victim-sensitive policy recommendations that promote the inclusion of victims’ voices in police BWC policy.

William Daniels:

‘Surveillance in the City: From Surveillance Capitalism to Racial (Surveillance) Capitalism’

The question of surveillance capitalism has been recently debated in the fields of Information Technology and Consumer Behavior, with scholars such as Shoshana Zuboff arguing that personal information in the digital age has been increasingly commodified. However, this scholar has not addressed the question of how the commercialization of surveillance is connected to Cedric J. Robinson’s concept of racial capitalism. Specifically, in my paper, I will be looking at how surveillance functions in a majority African American city such as Detroit, Michigan by analyzing the Project Green Light program, which is a public-private partnership instituted by the Detroit Police Department, which installs high definition surveillance cameras with real-time facial recognition technology, that connects the cameras from businesses such as, gas stations, liquor stores, and fast-food restaurants, directly to the police headquarters. Building on the work of Simone Browne, which illustrates how racializing surveillance impacts black geographies, I contend that the surveillance of racial minorities in rapidly gentrifying spaces is deeply connected to neoliberalism, racial capitalism, and surveillance capitalism.

Police & Intelligence

Moderator: Ayla Zehtab-Jadid

Scott Thompson:

‘Charting Police ‘Street Check’ Dataflows and the (Re)Organization of Work in a Northern Canadian Prairie City: Or, You Can’t Just Move to Moose Jaw and Everything Will be Fine'

Drawing on a complete five-year dataset of police ‘Street Checks’ conducted in a Canadian prairie city (N=1,657), this empirical study demonstrates how knowledge produced through this practice of ‘Carding’ (‘Stop and Account’ / ‘Terry Stops’) contributes data to, and draws data from, a much larger assemblage of interconnected government and private agencies. Specifically, this paper: i) quantifies the amount and kinds of data that, as a result of Street Checks, the police service within this study contributed to the larger assemblage; ii) it quantifies the kinds and amounts of data drawn from other organizations and then were incorporated into police Street Check files; and iii) it identifies for what purposes the police service used data from other organizations within their Street Checks. Ultimately, this paper demonstrates how moving to the remote community of Moose Jaw will not allow you to escape the disappearance of disappearance, but more importantly it shows, with empirical evidence, how and where Street Check data are currently flowing, and how, within these data, the views, understandings, and biases of front-line police officers are also flowing, shaping, and (re)organizing social interactions across the Canadian prairie provinces.

Phil Boyle:

‘Out of Order: Excavating the Surveillance of Infrastructure/Infrastructures of Surveillance'

Monitoring threats to critical infrastructure is a key component of Canada’s 2009 National Strategy for Critical Infrastructure. This surveillance capacity comes largely in the form of security intelligence, which is materially instantiated in practices such as lists, briefs, assessments, metrics and so on that are circulated amongst a range of partners symbiotically engaged in the ongoing security project that is critical infrastructure resilience. Based on an excavation of federal archives dating back to 1948 this presentation will show how this intelligence infrastructure emerged out of the failure of an antecedent federal program that sought to enumerate industrial facilities necessary to wage industrial war. While the socio-legal transformations that underpinned this failure were premised on securing the post-Cold War social order, they simultaneously augured the formation of new forms of surveillance fixated on revealing human collectivities deemed to be ‘out of order.’

Martijn Wessels:

‘How algorithmic policing configurations determine accountability risks: the development and application of a sociotechnical model’

The digitalization of surveillance by policing organizations is evolving towards the utilization of algorithms and artificial intelligence to support or replace human agency. The algorithmization can be seen in both predictive surveillance technologies in which historical (big) data is being used to extrapolate future offences, as well as in real-time applications in which policing organizations are invested in recognizing patterns of (potential) misconduct through technology, to act pre-emptively or to improve their reaction time. This trend sparks new questions and challenges regarding its societal and organizational consequences. This study widens the debate on the algorithmization of surveillance by structuring the consequences for both real-time and predictive applications in different sociotechnical configurations. Through a systematic literature review of academic literature on the algorithmization of surveillance in The Netherlands and the United Kingdom, this study showcases how scholarly attention is dispersed, what the differences are between both policing contexts, and what the contemporary challenges and risks are in respect to this algorithmization trend. This study concludes by providing avenues for how these challenges and risks can be addressed by future research.

Policing Technologies

Moderator: Catherine Stinson

Sanja Milivojevic:

‘Voyage(r) into uncertain future: New frontiers in surveillance on social media'

Predictive policing (or ‘crime forecasting’) is the flagship of algorithmic governance and the key catchphrases of police practitioners (Wilson, 2018). It first gained traction particularly in the major cities in the United States. Today, crime prediction is ‘the new watchword for innovative policing’ (Ferguson, 2017: 1112). The idea behind this ‘smart’ crime forecasting is that by using big data, both crime and not crime related, we can identify not only probable future crimes and where they are likely to occur, but also likely offenders and victims (Perry et al., 2013; Wilson, 2018). Welcome to the era of pre-crime, in which agencies of social control aim to disrupt, incapacitate, restrict and ultimately punish future crime threats that may never materialise (McCulloch and Wilson, 2015). Policing that rests on "traditional" methods of crime prevention is increasingly replaced with numerous practices of technocratic crime forecasting. Small artificial intelligence (AI) start-ups are emerging players in this growing and lucrative field. This paper looks at one such actor, the company called Voyager Labs that aims to scan your friends on Facebook or Instagram posts and in so doing assess your likelihood of offending or recidivism. The company's moto is: 'Make the invisible visible'. This paper theorises just how problematic this and similar AI-based approaches in 'new policing' are, and what we need to do to resist them.

Allison Holmes:

'Disproportionate by Default: Digital Data Extraction and the Investigation of Sexual Offences'

In the investigation of sexual offences, digital evidence is a key element and its acquisition can be critical to a successful prosecution. While access to an alleged offender's data falls within the remit of investigative material, there is increasingly a demand to subject victims to intrusive digital examinations. Such measures subject victims to enhanced scrutiny, reinforcing power disparities between the victim and the state. This paper analyses the risk posed to victims' rights in these so called 'digital strip searches' wherein details of their private lives are laid bare. In order to assess the necessity of these measures, the paper takes a comparative perspective, looking at both UK and EU policy and the existing safeguards governing the acquisition and disclosure of this evidence. It is argued that the requirement for victims to consent to intrusions into their privacy in order to obtain justice represents a further violation of their personal autonomy. These measures make access to justice contingent on individuals' willingness to subject their lives to intrusive surveillance practices. Through an analysis of the criminal evidence processes which govern digital disclosure and the portrayal of digital evidence in the criminal process, this article argues that the current regime represents a disproportionate interference with the right to privacy life and posits reforms to ensure that victims' rights are guaranteed in the investigation and prosecution of sexual offences.

Laura Neiva and Helena Machado:

'Big Data technologies for criminal surveillance purposes: How to promote transparency and ethical debate'.

This paper reflects on the use of Big Data for criminal surveillance purposes and its potential to trigger disempowerment effects, understood as negative social consequences on individuals, groups, and societies. The application of Big Data to surveil and identify criminal suspects involve: (i) the opacity of technologies in terms of their implementation and use; and (ii) the permanence of racialized and discriminatory practices. We consider the guidelines for responsible innovation and anticipatory governance of technologies to argue about the need to promote an interdisciplinary and collaborative debate on implementation of Big Data for criminal surveillance purposes. Following an approach based on the deliberation of three values – robustness, usefulness, and legitimacy – we explore the need of promoting awareness around the errors and biases of the technologies, their (dis)advantages, and their moral and ethical costs. Oriented towards public involvement in deliberations on the legitimate uses of technologies makes it possible to reinforce principles of accountability and transparency, inclusion and social equality, and trust and democracy. These debates are required, especially – as in the use of Big Data to criminal surveillance – when the technology comes to inform decisions of the criminal justice system.

Dean Wilson:

'The New Platform Policing: Data and the Maximal Officer'

The infusion of information technologies within policing ecologies has accelerated considerably since 2008. Frequently this is couched in the language of efficiency and of enabling police agencies to do more with less. While engaging various models including the notion of software as a service, the valence is towards cloud-based information architectures that infuse police organizations and which meld together disparate sources of data into modulated flows of maximal utility. While much reference is made in marketing materials to Artificial Intelligence (AI) and machine learning, these new digital policing ecologies also engage with a lineage of policing techniques, such as hot-spot policing, which have considerably longer historical trajectories. This paper examines the emergence of 'platform policing', arguing that it draws upon imaginaries of efficient and cost-effective law enforcement that have their origins in the US context of the 1960s. Efficiency is imagined as emanating from intense datafication and surveillance of the body of the police officer, which becomes a key node of data flows. Platform policing also envisages police agencies that are lithe, flexible and constantly adjustable. Importantly, it also positions police agencies as a key consumer and co-producer within 'platform capitalism', in the process enacting processes of economization.

PANEL: Surveillance & Police Body-Worn Cameras: The Past, Present, and Future

Panelists:

Amanda Glasbeek
Alana Saulnier
Tjerk Timan
Bryce Newell (Chair)

Police agencies (and other public bodies) in various countries have been adopting modern body-worn camera technologies for over a decade now. A quickly growing body of research, within criminology and an array of other disciplines, has begun to shed light on what the adoption and use of these devices means for police work and for broader society. Police adoption of body-worn cameras has been motivated by different concerns in different parts of the world, ranging from police transparency and oversight to police safety and evidentiary benefits, among others. However, the surveillance-related implications of body-worn camera adoption is a shared concern. Regardless of whether cameras are adopted with the stated aims of calming civilians and ensuring the safety of public employees, producing useful evidence, or providing greater police transparency and accountability, body-worn cameras are tools of surveillance. They are tools of techno-regulation, where police officers and civilians are being watched to promote behavioral change. The use of the cameras is about exerting power, about social control, and about using the data/information/evidence generated to preserve and enlarge the power of the state. As a technology, body-worn cameras are also just a starting point. As biometric identification, artificial intelligence, and high bandwidth wireless technologies (e.g., mesh networks, 5G) are incorporated into the body-worn camera ecosystem, the surveillant power of these technologies will increase dramatically. Thus, we need to have serious discussions about the surveillance-related implications of where we are now—and where we may be headed in the future—and what we can do about our present and our potential futures. In this panel, which will function as a roundtable discussion between expert researchers in both academia and private practice, we will explore these questions. The roundtable will be moderated, with a set of pre-determined questions to provoke initial discussion, and we will also open the discussion to questions and dialogue with the audience. Panelists include experts with experience researching body-worn cameras within multiple countries.

PANEL: Digital Technologies in Policing & Security I

Digital technologies in policing and security are growing in use, especially those using predictive analytics and algorithmic assessments. With developments like predictive policing, terrorist risk profiling, recidivism risk assessments, and behavioral prediction for classified information holders, security-related practices are progressively based on new, algorithmic forms of knowledge production. While technology has always played an important role in matters of policing and security (Bain, 2016), the introduction of digital, algorithmically mediated technologies is accompanied by significant challenges. For instance, law enforcement agencies regularly do not know how algorithms are sorting information (Dencik, Hintz, & Carey, 2017), and algorithms often present a false cloak of scientific fact (McCulloch & Wilson, 2016). These two panels explore issues emerging from the use of digital technologies in policing and security and engage in the conference themes of targets, tracks, and traces by exploring who law enforcement pays attention to, their methods of use, and their lasting impacts.

Panelists:

Vlad Niculescu-Dinca

Joery Matthys

Nikolaus Poeöchhacker, Angelika Adensamer, Peter Kahlert

The first panel theorizes surveillance, offering a conceptual framework for analyzing the digital technologies in policing and security. It also provides a framework to analyze current and projected developments in technologically mediated surveillance, examines the state of legal technologies, and critiques calls for oversight.

PANEL: Digital Technologies in Policing & Security II

Panelists:

Fieke Jansen
Sarah Young
Ciara Bracken-Roche
Vlad Niculescu-Dinca (Chair)

The second, empirically oriented panel offers insights into digitally mediated data-driven practices by articulating the intricate ways in which surveillance subjects are already rendered visible and thus informing the debates around unfair and unjust interventions enabled by these practices. The presenters examine the practice of data-driven individual risk assessments in policing, AI-based classification of online hate speech, and showcase a trend towards datafication of policing in Germany, the Netherlands and the UK.

PANEL: Predictive Policing

Panelists:

Gwen van Eijk
Kelly Vink
Quirine Eijkman
Pieke de Beus
Frederik Zuiderveen Borgesius (Chair)

Predictive policing tools have proliferated in the last two decades as an answer to increasingly louder calls for more effective, efficient and objective policing. Predictive policing concerns the use of automated predictions about who will commit crime or when and where crime will occur. Predictive policing has been hailed as a step towards forward-looking crime prevention and more legitimacy, but it has also been criticized for its potential discriminatory effects, in both design and daily operation. One of the problems is that predictive policing can discriminate unintentionally, for instance when an algorithm learns from data reflecting biased human decisions. Second, profiling-based decisions are often incorrect for a particular individual. Profiling typically entails applying a group profile to individual cases. Third, profiling is opaque: people may not know why they are treated differently. Making profiling transparent is difficult, among other reasons because of the complexity and the possibly ever-changing nature of algorithms. This panel is a lively discussion panel: no long presentations, and slides are prohibited. We will have a discussion among the panellists and with the audience. We can discuss questions such as:
- Does it make a difference whether predictions are made about people or about streets?
- Are there circumstances in which predictive policing should not be used?
- What are the risks of unfair or illegal discrimination, if any?
- Do the advantages, such as efficiency, outweigh the disadvantages, such as the risk of discrimination?

Data Sharing Partnerships & Supply Chains

Moderator: Catherine Jasserand

Maja Dehouck and Marieke de Goede:

'Financial Information-Sharing Partnerships as Financial Surveillance: Legal and Ethical Implications'

The global response to terrorism financing and other financial crimes hinges on financial institutions who are authorized to fulfill the role of security actors. They monitor payment transactions, close accounts, mine their databases and report on suspicious or unusual transactions by their clients (de Goede, 2018). These practices have gained scholarly attention as a form of financial surveillance, demonstrating their ethical implications, unintended consequences and lack of effectiveness. In recent years, Financial Information-Sharing Partnerships (FISPs) have emerged as a more targeted alternative to these large-scale forms of financial surveillance. These partnerships entail novel forms of pro-active data-sharing between public and private institutions, at the limits of law. They involve new ways of identifying and tracking targets of suspicion. However, due in part to their promise of a more targeted approach to financial intelligence, important questions regarding their legal and ethical implications so far remain overlooked by academia and practitioners. This paper mobilizes literatures in Surveillance Studies to analyse FISPs as an emerging form of financial surveillance. It offers a critical analysis of the data practices of FISPs and raises questions concerning the ways in which they target and track citizens. By challenging the privacy implications, democratic legitimacy, potential for mistakes and misuse, proportionality and accountability structures of FISPs, this article maps out a new problem space in the study of financial surveillance.

Aaron Martin:

'Humanitarian Data Analytics: The problematic case of the World Food Programme's partnership with Palantir

In 2019, the UN World Food Programme—one of the largest humanitarian agencies—announced it would be partnering with the data analytics firm Palantir to help streamline WFP's delivery of food and cash-based assistance across its global operations. Civil society reacted to question whether Palantir would be able to access sensitive information about WFP's beneficiaries, while also raising concerns about Palantir's business model and the risks of technological lock-in and bemoaning the lack of transparency surrounding the agreement (Easterday, 2019). The partnership has also exposed tensions at the intersection of privately-provisioned humanitarian technology and state sovereignty: WFP's operational data provides Palantir with deep insights regarding food in/security in countries affected by crises. Palantir's access to this information has heightened concerns among states about the involvement of a private technology firm with strong ties to the US security establishment in sensitive humanitarian work (Martin et al., 2022). Building on these previous analyses, this paper presents an in-depth case study of the WFP-Palantir partnership based on publicly available information (e.g. press releases, annual reports, etc.) and interviews with key informants over the past two years, and explains why the case presents novel problems for surveillance scholarship (i.e. the supply chain optimization objectives make traditional privacy critiques less compelling).

Gabriel Grill:

The politics of data in labor unrest risk assessment across global supply chains

The wide availability of online publicly accessible data sources, such as social media, news articles, and other sensor data, has motivated governments and corporations to invest in algorithmic risk assessment tools to detect and anticipate protests and labor action. Their stated goal is to more effectively minimize the impact of unrest activity within supply chains and deploy law enforcement and security assets to preempt disruptions to governmental and corporate operations, but these systems raise serious concerns for human rights, surveillance, and the future of democratic participation and labor organizing. In this paper, I discuss the affordances and promises of such civil unrest risk assessment and prediction technologies by conducting a socio-technical analysis of methods and different types of data used. The analysis draws on data science research papers, and other relevant public documents detailing socio-technical aspects of Unrest Detection and Prediction (UDP) systems. The methods described in the documents range from simple logistic regression to less interpretable deep learning approaches that combine quite diverse inputs (such as financial indicators, weather forecasts, social media posts, and some even reservation cancellations). Furthermore, new kinds of variables and features are extracted from these online data sources, such as affect in language use and information propagation strategies on social media (Grill, 2021). My analysis highlights specific perspectives and politics enacted by these data, shows a need for globally oriented regulation centering worker rights across supply chains and calls on global labor movements to pay attention to new forms of networked digital surveillance.

Platforms
Moderator: Linnet Taylor

Somto Mbelu and Payal Arora:

'Ethical Concerns in Designing AI-enabled, Health Insurance Platforms in Nigeria

Many African health systems have inadequate financial risk protection for their health consumers, requiring most patients to pay for health services out of their own pocket (OOP), putting them at risk of financial ruin. According World Bank, (2015) 11 million Africans are falling into poverty every year due to high OPP. Sub-Saharan Africa has among the world's lowest levels of Universal Health Coverage (UHC) due to underutilization of services as well as poor access to quality healthcare, thereby negatively influencing Africa's health indices. With global advances in information and communication technologies (ICTs), efforts are now being made to ensure the continent makes progress towards its UHC goals by leveraging the relatively new technological applications of artificial intelligence (AI) and machine learning (ML) to deploy healthcare initiatives. AI has become a powerful tool to reshape human interactions and environments. According to Jiang et al., 2017, AI can be used to obtain insights to assist in providing quality clinical practice. AI platforms extract valuable evidence from large patient populations to make real-time inferences for health risk alerts and health outcome predictions. As the need for AI-led healthcare insurance systems continue to emerge in Africa, it is pertinent to develop strategies and guidelines for the design and deployment of these platforms to ensure they provide an all-inclusive, fair, and transparent system for all. As health-tech organizations continue to design AI-related innovations to advance UHC goals in Africa, questions on the existing models of UHC and how to best pioneer a model that works best for the context and conditions of sub-Saharan Africa need to be addressed considering the non-existent or nascent privacy and data protection laws in these contexts (Arora, 2019). In Nigeria, regional governments in partnership with private tech companies have commenced the deployment of AI-enabled digital platforms to address the problems of a dearth of health actuaries, inadequate risk modelling, and inadequate resource generation and allocation of funds for insurance. To ensure quality and affordable healthcare delivery via AI digital health platforms it is imperative that strong ethical regulations and guidelines are set in place to ensure users of these platforms are not exploited, thereby ensuring the ethical uses of health data for the benefit of society. The purpose of this study is to contribute to the existing body of knowledge on the topic by focusing on the ethical concerns for designing AI-enabled Health Insurance Platforms in Nigeria. It will investigate the role AI and mobile technology can play in evaluating risk, enabling access, thereby reducing costs for Health Insurance for the underserved, while advancing the tenets of UHC in Nigeria. It will also explore best ethical framework for the facilitation of ethical uses of health data for the benefit of society. This paper employs qualitative content analysis and a comparative case study of 4 basic Health System Models. These include the Beveridge, Bismarck, National Health Insurance and Out of pocket model. This analysis will compare and outline the best fit model for the Nigerian context.

Rocco Bellanova, Ronan Ó Fathaigh and Judith Möller

Digital Platforms and the Digitisation of Government Surveillance'

Over the past five years, governments have been able to leverage the power of platforms to impose new forms of restrictions on free expression, and engage in the surveillance of individuals and online activism. Platforms are now expanding cooperation with authorities, including sharing data about users flagged by law enforcement and other authorities. These forms of platform/government cooperation raise multiple concerns. Moreover, platforms are becoming both tools of government and targets for regulation, and taking advantage of regulation by platforms. This paper examines how European governments are leveraging the power of digital platforms to engage in government surveillance online, and assesses the compatibility of these measures with European human rights law. The paper applies a unique interdisciplinary perspective, bringing together law, political communication and surveillance studies. First, the paper examines how platforms' algorithmic systems shape (and limit) information dissemination. The paper then critically analyses EU-based government-platform initiatives that exist to surveil citizens and gather information. Third, it assesses how these measures comply with freedom of expression and the right to privacy, and concludes with recommendations on remedying problematic elements of the role platforms play in digitisation of government surveillance.

Kathrin Friedrich and Sebastian Randerath:

On track: Space-time critical entanglements of delivery platforms'

Platform-based tracking entangles space-time critical operations of different actors. In particular, tracking in gigwork such as food delivery entails processes of dataveillance, geotagging and work capture directed towards capital accumulation. How can these sociotechnical entanglements of heterogeneous tracking operations be critically analyzed? In our contribution we will map different conceptual and methodological levels of platform-based tracking from a media studies point of view to show how surveillance practices unfold and gain force beyond digital environments. We will take a German delivery platform as a case study to investigate different tracking operations in a mixed method approach. This approach combines a walkthrough analysis of the platform's drivers app with a media ethnography. Thereby, we identify space-time critical entanglements on different media theoretical levels. We aim to show how a media studies focus on tracking operations can make a crucial contribution to the analysis of sociotechnical entanglements in contemporary surveillance practices by examining tracking both "from below" through an ethnographic observation of workers and unions and "from above" through a walkthrough analysis of the algorithmic management of the platform itself.

PANEL: Researching the Rise of Employee Monitoring Applications

Panelists:

Phil Boyle (Chair)
Adam Molnar
Krystle Shore
Xavier Parent-Rocheleau
Ariane Ollier-Malaterre
Luc S. Cousineau
Danielle Girard
Morgan Banville

While the use of surveillance technologies for 'employee monitoring' has always been contentious, the shift toward remote working, amplified by the COVID-19 pandemic, adds urgency to understanding the implications of employee monitoring software. A greater number of businesses are now seeking ‘off-the-shelf’ software applications to monitor and manage remote workforces—relying on features like keystroke logging, webcam usage, and time-tracking—for the stated purposes of enhancing worker productivity and minimizing cybersecurity risks. The seismic culmination of an increasingly remote workforce and the emergence of digital apps that monitor a range of employee activities, raise novel questions related to workplace privacy, social control, and the ongoing impacts of AI-driven surveillance and modelling for work and labour. This panel will discuss the phenomena of workplace surveillance through the narrower prism of the proliferation, use, and impacts of employee monitoring applications. A diverse range of disciplinary and theoretical perspectives, including critical political economy, organizational management, cultural studies, law, and sociology will inform discussions about: (i) how scholarly disciplines have structured knowledge about workplace surveillance and to what effect, (ii) empirical quandaries of 'old' and 'new' forms of employee monitoring and how this informs privacy and social impacts, and (iii) how companies justify their use of employee monitoring apps in today's era of remote work. This panel also (iv) invites surveillance scholars to reflect on the practice of researching employee monitoring applications and (v) will prompt discussions of the prospects and limitations of advancing interdisciplinary methodological strategies that draw from disciplines such as computer science to assist critical inquiry into employee monitoring applications. As such, the panel will be of broad concern to conference participants interested in how mixed methods approaches that draw together critical disciplines such as social science, computer science, and law, can be leveraged in the study of monitoring applications more generally. The proposed format of this panel includes four presentations on various workplace surveillance trends and associated methodologies (see associated information). This will be followed by a broader discussion led by the chair on the prospects and challenges of 'doing interdisciplinary work' on employee monitoring applications.

PANEL: Surveillance Studies & the Global South

Panelists:

Azadeh Akbari (Chair)

Fernanda Brunoanna

Linnet Taylor

Rodrigo Firmino

Silvia Masiero

The panel, "Surveillance Studies and the Global South," aims to initiate a discussion on the importance of integrating the global South in shaping the scholarship on surveillance studies. Representatives from Research Network Surveillance in the Global South, Latin American network of surveillance, technology and society studies (LAVITS), IFIP 9.4 (working group on the Implications of Information and Digital Technologies for Development) and Global Data Justice Group at Tilburg University will introduce their affiliated groups shortly and then enter a discussion on the reasons behind focusing their research and activities on the Global South and its significance for surveillance studies. The discussion will be facilitated by the panel's chair. Research Network Surveillance in the Global South debates the absence or underrepresentation of research, experiences, trends, concepts, theories and knowledges from the global South in the universalising discourse of the Western-centric field of surveillance. The network, therefore, aims to build a space of exchange between researchers that situate their point of view in the global South. The International Federation for Information Processing (IFIP) Working Group 9.4 was founded in 1988 to explore the potential of information and communication technologies for social good. The group grew into a network with an interdisciplinary, largely critical focus on ICT for development (ICT4D), in which multiple aspects of engagement of technology with "development" are explored. The group has recently started an active engagement with data justice and surveillance, which will be further pursued in the Conference. Created in 2009, LAVITS intends to be a regional exchange hub between Latin American researchers, activists, and artists. It is a multidisciplinary network that aims to encourage the production of critical knowledge, artwork and political action in topics involving surveillance technologies and practices. The Global Data Justice project focuses on the diverse debates and processes occurring around data governance in different regions to draw out overarching principles and needs that can push data technologies' governance in the direction of social justice. The project is based at the Tilburg Institute for Law, Technology, and Society in the Netherlands.

STREAM 6: MEDIA & COMMUNICATIONS

Public Attitudes, Influence & Information

Moderator: Tjerk Timan

Lin Pan:

'Dying Investigative Journalism in Surveillance Age'

Scholars focusing on the watchdog role of media in democracy normally take investigative journalism as a normative example. However, both investigative journalists in the UK and the US are caught in a predicament and even a crisis of survival in the mass surveillance era. A similar situation has been witnessed in the Chinese context. This research will explore the predicament of Chinese investigative journalism from the news source perspective which is regarded as the life-blood of investigative journalism. Unlike general news production, investigative journalism is more leak-oriented and it is responsible for source protection. Source use is different in the digital age, and it is deeply affected by the mass surveillance and chilling effects caused by that, thus hindering the production of investigative journalism in terms of seeking more leaks, investigation, and fact-checking. Thus the research aims to explore to what extent surveillance hinders the production of investigative journalism in China. This study adopts the method of content analysis, looking at the investigative reporting published from 2014 to 2018 from four media outlets in China. It attempts to observe the trend of sources use in the production of investigative journalism and has a better and in-depth understanding of the relationship between sources and investigative journalists in the Chinese context in the age of surveillance.

Qian Huang and Zhen Ye:

'Walking on eggshells: Influencer's everyday affective labour under watchful eyes'

Social media influencers benefit from the audience in the current attention economy, yet are also constantly scrutinized by viewers, leading to potential public shaming and boycotting. Unlike civilian users, it is hard for the influencers to withdraw from social media platforms, which is a common strategy to cope with online public shaming because online visibility is their source of social and economic capital. Therefore, we aim to understand how influencers cope with ubiquitous lateral surveillance and negotiate their daily production practices while maintaining online visibility. As a case study, we chose a Chinese Marvel fandom influencer who produces content on both Chinese and western social media platforms, including Sina Weibo, Twitter, and YouTube. This influencer experienced three major incidents of public shaming and many more minor ones. We conducted the longitudinal in-depth case study between 2018 to 2021 by utilising two sessions of 2-hour semi-structured in-depth interviews (in 2018 and 2021) and one week of assisted autoethnography in 2020. Our data shows that the influencer is forced to form strategies in response to the shaming in daily production practices of choosing words, content to (re)post, accounts to interact with, etc., which dramatically increase the affective labour required from the influencer.

Celina Van De Kamp and Scott Thompson:

‘Public Perceptions of Privacy and Privacy Protections in Metadata Collection, a Canada-Wide Public Opinion Survey: Is It Strange That Tim Hortons Wants to Know Who That Other Cup of Coffee is For?’

Working from a Canada-wide public opinion survey that links specific forms of metadata collection to feelings about privacy, this project demonstrates that there is a false understanding of the extent, intensity, and invasiveness of metadata collection by corporations and governments within the general public, and with it, a false sense that this collection does not violate the privacy of most Canadians. Specifically, this project moves beyond a simplistic "how concerned are you about metadata?" mentality, and instead links real world applications to public opinion regarding privacy and privacy protection. Results identify variation in responses to the comfort and discomfort of metadata collection, when there was specific uses that could be justified, versus blanket collection, as well as what type of organization was collecting the data. Additionally, a strong understanding exists for those polled that greater privacy protections should exist in Canada. These results speak directly to the need to recognize that privacy laws require an update to fit public understandings of data collection and their expectations of the protection of their privacy.

Lukas Antoine:

‘Costs, inconvenience, or civil rights? Investigating determinants of public support for surveillance’

The rapidly changing world creates actual or perceived insecurities for many people. As a response to security threats, governments around the globe, albeit in different magnitude, have implemented measures of mass surveillance. Regardless of prominent (normative) debates on surveillance and security, studies examining individual attitudes and factors explaining them has been relatively scarce. While people in general prefer living in a secure environment, we argue that it is not only the imminent trade-off between security concerns and protecting one’s privacy and freedom that ultimately persuades citizens to support surveillance measures. We expect that the support of such policies also depends on financial costs, their impact on individual convenience, the design of the policies as well as the context in which they are implemented. With the underlying study, we contribute to the literature by increasing our understanding of what makes people agree to proposed security measures and how efficient they perceive them to be. Using a factorial survey experiment, we measure the causal effects of the threat level, the strength of privacy interventions, financial costs, and time resources on the approval of security measures and their expected efficiency. The pre-registered experiment was conducted with 5,000 respondents in Germany. Results show that German citizens are in general willing to accept the introduction of far-reaching surveillance measures, but that related financial costs and individual convenience significantly influence such support. Context, in this case whether a safety threat is salient, however, has no effect on individual support.

Shaul Duke:

‘Deciphering Apathy Towards Surveillance: Nontargets as a Key Concept'

Public apathy towards surveillance is one of the greatest dilemmas of both surveillance studies and privacy-related scholarship. Among other things, it is what produced the “privacy paradox”, a concept that rose from the observation that individuals do not seem to take the necessary and readily available steps to assure their own privacy, at times even in cases when they declare that they are concerned about privacy. Moreover, even those studies that showed how individuals do take steps against their own surveillance, usually presented activism with regards to lateral surveillance, and much less towards top-down surveillance. In this talk I will argue that in order to understand this observed apathy towards surveillance we need to break down the category of “public” into subgroups, and to assign each subgroup either the label target or nontarget. Once we do this, a variance in degrees of apathy appears, and a large part of this previously uncomprehensive apathy is explained. The concept of nontargets, and its effectiveness in explaining public reaction towards surveillance will be exemplified by the apathy displayed by the Israeli public towards the (globally unparalleled) use of the secret service (Shin Bet) to do COVID-19 contact tracing.

Rights & Resistance

Moderator: Gerard Ritsema van Eck

Lauren Kilgour:

‘Resisting Stigma, Critiquing Surveillance: The Personal Resistance Practices of People Required to Wear Electronic Ankle Monitors’

In this article, I describe the ways that people required to wear electronic ankle monitors engage in the important everyday cultural work of resisting the stigma that wearing an electronic ankle monitor invites into their lives. Specifically, I discuss the ways that people who have been, or are, required to wear electronic ankle monitors use social media, broadly construed, to present new narratives about electronic ankle monitors and wearers that resist the stigmatized meaning associated with ankle monitors versus resisting their mechanical operation. I argue that these efforts represent important reclamation work around the continuing stigmatization of the social category of “the criminal.” Working towards a more just future of technology design and use urgently depends upon centering and elevating the voices, acts, and experiences of people and communities rendered vulnerable by technology design and deployment. As this research shows, addressing the harms of surveillance technologies requires studying both their data-based facets as well as their aesthetic, visual properties.

Jessica Ramos:

'Out of the Shadow: A Case Study On Oakland, California Resistance Against Policing Technologies'

Oakland, California has actively embodied resistance. Through the establishment of the Oakland Privacy Advisory Commission, Oakland became a model towards the resistance against new and existing technologies used within the city. They have a private commission that brings existing technologies out of the shadows and into a space where members of the commission, law enforcement, and the public all come together to discuss transparency and regulation. Prior to the establishment of the Oakland Privacy Advisory Commission, technologies were deployed within the City of Oakland with no regulation, discussion, or transparency. It is vital to understand that the commission does not completely abolish existing or new technologies deployed within the city. However, they set the discussion stage and through policy hold the executor of the technologies accountable. The Oakland Privacy Commission holds power in resistance and has forced accountability and a push towards transparency in limiting the use of technologies. Overall, this research seeks to examine through a case study of Oakland, California the local resistance embodied by the Oakland Privacy Advisory Commission in mapping out full transparency and regulation of two technologies: Cell-Site Simulators and Automated License Plate Readers.

Peter Ullrich and Philipp Knopp*:*

'Protest under Surveillance: Security Cultures and the Spiral of Surveillance and Counter-Surveillance'

Police forces selectively confront social movements with repressive and preventive surveillance measures. Analyzing 12 focus groups on video surveillance at demonstrations with different groups of protesters, participant observations, and document analysis with a Grounded Theory Design, we developed on the notion of "security cultures" in social movements. Security cultures are "collective sets of practices and interpretive patterns aimed at securing safety and/or anonymity of activists as well as making their claims visible. Thus, they are productive power effects, resulting from the very conditions under which protest takes place in contemporary surveillance societies." (Ullrich and Knopp 2018). The concept insists that it is not possible to understand protest without analyzing its involvement with police and surveillance. Security cultures are drivers of differentiation among protest groups, of protest repertoire changes, and, finally, they mold protesters' (collective) identities and perceptions of the state and society. Security cultures emerge within the conflictual "arms race" between surveillance and counter-surveillance (Gary T. Marx 2009) that has long been untangled from seemingly fixed positions of police monitoring and monitored protest. Ultimately, the concept complements basic notions of surveillance studies (spiral of surveillance and counter-surveillance) and uses their potential to better understand police-protest-relations.

Social Media

Moderator: Fareed Ben-Youssef

Alessandro Caliandro, Guido Anselmi, Veronica Moretti and Guido Legnante:

‘Mapping the culture of surveillance capitalism on Twitter through Digital Methods’

Although surveillance capitalism is already well-established in advanced economies, we can argue that the current Covid-19 emergence has probably accelerate the diffusion of surveillance capitalism logics and infrastructures (e.g., platformization of higher education). Despite the pervasiveness and currency of this phenomenon, we still know very little about how the general public perceives and frames it. In particular, there is a shortage of empirical research on citizens’ opinions towards surveillance capitalism as well as their level of awareness about the processes of data exploitation and value extraction carried out by corporate platforms on the very data users produce through their everyday digital practices. To address this research gap, we developed an exploration (based on digital methods) on dataset of 302k Italian tweets – (collected by following ad hoc keywords, such as ‘surveillance + Facebook’, ‘surveillance + iPhone’, etc). We analyzed this dataset combining computational and qualitative techniques – network analysis, topic modelling, ethnographic content analysis. Our preliminary results show that, on a general level, Twitter users seem unable to distinguish between processes of surveillance upon citizens and consumers (which they consider basically the same thing). Anyhow, on a micro level, specific communities of users tend to develop different narratives on surveillance capitalism, imagining different ‘models’ of it (such as, dystopian surveillance, benevolent surveillance, conspiracy surveillance, entertainment surveillance).

Guido Anselmi, Veronica Moretti and Alessandro Caliandro:

‘Every breath you take, I'll be watching you. (Un)making sense of algorithmic through countersurveillance measurements in the healthcare’

Vocal assistants based on AI technologies (like Alexa) can be considered the as the ultimate devices of surveillance capitalism, given their capacity to penetrate the more intimate spheres of consumers’ everyday lives. Different studies started investigating this phenomenon, focusing on different key aspects, such as privacy issues (Pridmore et al. 2019), datafication of emotions (Ball & Webster 2020), perceived utility and drawbacks (Puntoni et al. 2021). Nevertheless, studies on the culture of surveillance (Lyon 2017) unfolding around these AI devices is still scarce. To address this research gap, we developed a quali-quanti analysis of 5197 Facebook posts containing the keyword ‘Alexa’. Following Lyon, we explored the culture of surveillance by mapping users’ imaginaries and practices of surveillance (Lyon 2018) - paying particular attention to the everyday strategies through which they engage with surveillance (responsive, initiatory, negotiatory). Furthermore, we expanded the Lyon’s model by combining it with some inputs from human-machine communication theory (Guzman 2019). Drawing on Guzman and Lewis (2020) we analyzed users’ narrations on Alexa (and its surveillance capacities) by focusing on the 3 key communicative dimensions of AI (functional, relational, metaphysical).

Daniel Trottier and Frazer Woodhead:

‘Norm enforcement on Reddit: Rules of engagement and participation'

The social platform Reddit hosts a set of online communities that denounce offensive behaviour, invoking scrutiny and shame on (categories of) individuals. Despite varying in their targets, they all promote actionable content to an audience who can view, share and comment on it. These groups allow a global public to air grievances, enabling both accountability and abuse. Following high profile privacy and reputation scandals, Reddit routinely sanctions and purges actionable 'subreddits'. As a matter of self-preservation, subreddits that watch over the public also maintain heightened (self-)scrutiny of its own members. Group rules and other de- and prescriptive texts are a means to instil this scrutiny among a broader audience. In analysing rules and other content management practices in 65 scrutiny and shaming based subreddits, this paper considers how these groups temper platform-based surveillance.

David Myles, Stefanie Duguay and Lucia Flores Echaiz:

'Unpacking the social implications of AI-supported platform surveillance for the LGBTQ+ communities'

Digital platforms have introduced datafication and algorithmic infrastructures that are criticized for supporting pervasive surveillance schemes (Wood & Monahan, 2019) and reproducing inequalities among marginalized populations (Noble, 2018). Today, little is known about the social implications that AI-supported platform surveillance raises for the lesbian, gay, bisexual, trans, and queer (LGBTQ+) communities. This paper maps and analyzes a series of public controversies pertaining to LGBTQ+ algorithmic surveillance through a scoping review of the scientific literature and of magazine/newspaper articles. Informed by critical platform studies and feminist technology studies, it discusses three main trends: 1) Sorting algorithms predict and classify LGBTQ+ user identities through gender and sexual inference work, which results in new queer data publics that respond to commercial imperatives; 2) Recommendation algorithms have become new curators of LGBTQ+ cultures that mediate queer taste and cultural preferences; 3) Filtering algorithms are increasingly responsible for assessing what is deemed socially acceptable or valuable online, giving way to new forms of queer censorship and algorithmic resistance. Beyond algorithmic oppression, this paper concludes by reflecting on the productive nature of AI-supported platform surveillance and its propensity to reshape LGBTQ+ cultures, kinship, and subjectivities in line with neo-Foucauldian approaches to algorithmic surveillance (Bucher, 2018).

Vigilantism & Community Surveillance
Moderator: Joana Fonseca

Philipp Knopp:

'Keeping the police in the game: vigilance, activation, and normalization of emergency calls in Austria'

Emergency call processing is one of the most frequent ways to connect "peer-to-peer surveillance" (Andrejevic 2004) with state agencies. Relying on a critical discourse analysis of newspaper articles that issued Austrian police emergency call processing between 2010 and 2021, the presentation will argue that the activation for vigilance and mutual watching over is not an always extending process as dark visions of surveillance societies might suggest. Rather, I will show how state actors engage in controlling and normalizing vigilant activities. Critical theories of the “activation society” (Lessenich 2008) and normalization theory (Link 2013) will inform an interpretation of discourse that allows to understand the dialectics between unleashing and controlling citizens’ surveillance as a way to handle a central paradox of late modern policing: the legal obligation to persecute every perceived serious threat and the necessary selectivity of police practice. An overload of people’s surveillance activity, therefore, threatens the police as an organization and needs to be normalized. The presentation shows how – especially in times of crisis – the Austrian police tried to control vigilance in order to remain a relevant actor in people’s in/security practices.

Lior Volinz and Lucas Melgaço:

‘From Participatory to Lateral Surveillance: Municipal Apps as Platforms for Digital Informants’

Municipal apps prompt citizens to report incidents of urban disorder and nuisance in a rapid and simple manner, directly from their mobile devices to the relevant municipal department. However, these same platforms also allow individual citizens to anonymously report one another for minor criminal offenses, such as vandalism, graffiti, public urination, parking violations, or illegal trash dumping. Focusing on FixMyStreet, a municipal app used in Brussels (Belgium), this paper draws on a mixed methods research, including a content analysis of the incidents’ database and semi-structured interviews with municipal officials to explores how the introduction municipal apps contribute to the making of digital informants - and how this process risks extralegal vigilantism, ethnic profiling, privacy infringement, exacerbated neighbours’ feuds or diminished social cohesion. We delve into the function creep associated with municipal apps, in which participatory surveillance schemes, intended for local authorities to collect information on the urban environment, are transformed into spaces of lateral surveillance, where citizens surveil each other. We then continue to explore the different strategies employed by local authorities in response to demands by digital informants, and how concerns over inequity, limited resources and social polarisation subsequently shape municipal interventions.

Jossian Zoutendijk:

‘WhatsApp Neighbourhood Crime Prevention: a negative impact on perceptions of security?’

Like many Dutch cities, the city of Rotterdam propagates the use of WhatsApp neighbourhood watch by its inhabitants to make neighbourhoods safer. The expectation is that these digilantes will lessen crime, improve perceptions of security and strengthen ties with public service. But is that really the case? Studies do not provide us with hard evidence, but they do point to promising success factors. Can we make better use of these factors in order to meet expectations? A twofold experiment was conducted using a pre-test post-test design in which moderators of four WhatsApp neighbourhood watch groups carried out a set of interventions based on these success factors. Non-participating residents of the same neighbourhoods constituted the control groups. Three WhatsApp groups initiated and moderated by public servants of the city of Rotterdam were compared to a citizen initiated and moderated group. The moderators of all four groups applied the same set of interventions at their own discretion, with respect to the context of their group. The experiment partially unpacks the black box of WhatsApp neighbourhood watch in showing what interventions improve the efficacy under which circumstances. It also raises the question about the true function of these groups: improving security, perceptions of security or connectedness to peers or public servants? Could it be that a more expressive function has to be added to the equation?

Marielle Wijermars and Tetyana Lokot:

‘Surveillance tool or means of resistance? The Telegram messenger as a political actor in Belarusian contentious politics’

How do tech companies come to be seen as protectors of digital rights, and how do perceptions of their anti-surveillance safeguards impact their role in contentious politics? This paper examines the practices, performance and perceptions of the messaging platform Telegram in the context of the 2020 Belarus protests against election fraud, during which Belarus sought to restrict protesters’ use of digital technologies. Aiming to unpack platforms’ active role as part of surveillance infrastructures and their ability to impact political transformations, we examine how Telegram’s practices and performances, as well as the state’s and citizens’ perceptions of them, contribute to the platform’s reputation as both a tool of surveillance and a means of resisting it. The paper combines publicly available data from Telegram’s statements, media coverage, and a dataset of the largest local Telegram group chat affiliated with the 97% protest movement (Minsk). We find that Telegram’s performance and practices drive citizens to form affective connections to the platform and perceive Telegram as an ally in their struggle against repressions and digital surveillance. Meanwhile, the Belarusian state uses Telegram’s anti-surveillance stance to justify digital repressions, but also avails of the platform’s aversion to censorship to surveil protesters and engage in manipulations.

STREAM 7: SOCIETY & INSTITUTIONS

Bodies & Tracking and Education (1)

Moderator: Vlad Niculescu-Dinca

Lizzie Hughes:

‘Hearing Gender: reshaping surveillance as human, sensory, and (en)gendering through an analysis of sound in the public bathroom’

The gender-segregated public bathroom is a common-sense yet complex space. Within its walls, subjects are emboldened to enact various techniques of racialised gender surveillance. This paper will explore “hearing gender” as one such technique and, in so doing, offer a reshaping of surveillance as not just a method of monitoring but one of everyday (en)gendering. Typically, it is assumed that only trans and gender-nonconforming bodies are subjected to intensified surveillance within this site. However, by asking how gender is heard through sound, I will show that all subjects are involved in the monitoring and regulation of identities at individual and group levels, as well as (re)creating and embodying them in morphic and temporary ways in response to and in movement with the bathroom space. All subjects must aurally account for themselves through unnamed Whiteness, and bio-essentialist and classed acoustic channels that govern what “sounds like” a “real” woman or man – and therefore who counts as either, irrespective of claimed identity. This paper will touch upon questions of spatial belonging, affective surveillance, and the governance of gender. It will use queer and trans writing and emergent sensory criminology to make its claims, and call for further analysis of sensory surveillances.

Stefanie Felsberger:

‘Understanding Surveillance Capitalism through the lens of menstrual tracking'

The question of data commodification has found increased attention in recent years, and especially since the publication of Shoshanna Zuboff’s book ‘Surveillance Capitalism’ (2019). Much of the literature focuses on the activities of companies and leaves out the role of people: both the question of how to theorise the role of users in Surveillance Capitalism and how people navigate the commodification of their data. This ends up reinforcing the power of big tech but also reasserts the logic of (surveillance) capitalism. In my presentation, I ask how do users of period apps navigate the commodification of their data in the context of Surveillance capitalism and how can this contribute to the ongoing discussion about (surveillance) capitalism? First, I, explain why users of period trackers are a particularly interesting site to think about both surveillance, tracking, and capitalism. Second, I ask who uses these apps and why. I elucidate the consequences of period tracking for app users and other menstruators. Third, I ask does the constant self-tracking and subsequent data commodification reconfigure the boundaries between the market, the economy and the self and if so, how? My presentation draws from 30 interviews conducted with period app users in Vienna, Austria.

Andra Siibak and Kristjan Kikerpill:

‘Doom-Monitoring on Student’s Social Media: Schools and the Growing Surveillance Purview Creep'

Growing public concern about the safety and security of schools (Burke & Bloss, 2020), as well as students growing mental health problems (Schlitz, 2021) has led many schools to hire private companies to monitor students’ use of social media (Regan Shade & Singh, 2016). In short, the schools have started to engage in doom-monitoring i.e. they have extended and intensified technology-mediated surveillance practices of students under the justification of preventing the next “bad thing”, regardless of whether such actions actually achieve their supposed purpose (cf Burke & Bloss, 2020). The aim of our study is to explore how different participants engaged in the process – the students, the school officials, and the service providers – justify or condemn such surveillance on students’ profiles. We apply critical discursive psychology (Locke & Budds, 2020) to study news articles (N=295) from 2019-2021 reporting about the use of social media monitoring on students’ accounts that have been published in international media. Preliminary findings suggest that schools are practice doom-monitoring with the hopes of discovering potential harms that students may inflict on themselves as well as others, breaching thereby students’ interpersonal-, commercial-, and institutional privacy.

Kate Duffy and Ciara Bracken-Roche:

'Eye Spy 'Welfare Cheats': An Examination of Lateral Surveillance in Ireland'

This paper examines the role of surveillance by the Irish Department of Social Protection and Welfare (DSPW) with a primary focus on the 'Welfare Cheats Cheat Us All' Campaign. This campaign, launched in April 2017, is one of the most obvious manifestations of the DSPW's efforts to engage the Irish public in efforts to engage in surveillance and reporting of welfare recipients. The campaign is just one example of a series of neoliberal logics and policy changes to welfare programs and structures in Ireland, and while these have been engaged with by the academy, the role of surveillance and surveillance technologies has yet to be explored. Drawing on primary data collected through Freedom of Information requests as well as policy documents, legislation, and regulation, this paper explores a number of surveillance tools employed by the DSPW. The paper asks how surveillance of welfare recipients is conducted in Ireland with the case of the Cheats Campaign, as well as examining what kinds of ideas, norms, and beliefs shape the surveillance of welfare recipients. Through the lens of lateral surveillance (Andrejevic 2005), we argue that the DSPW and the Cheats Campaign encouraged direct surveillance and control of welfare recipients helped by criminalization and responsibilization. Hostile neoliberal logics result in the Irish government categorizing and controlling welfare recipients, as risks to be managed rather than individuals who need support.

Education (2)

Moderator: Gabriel Grill

Hayford Ayerakwa:

'Digital Literacy, Vulnerability and Surveillance among Grade 8 Students in Ghana'

Digital literacy has become important for individuals to actively participate in the global discourse. However, children and vulnerable groups need to be actively monitored to ensure they are protected. In a recent survey conducted among grade 8 students in Ghana, access to the internet in schools remained problematic. Students however indicated their ability to access the internet in their homes using android phones. The phones are used for different purposes including the search for educational content as well as sharing texts, images, or videos with family and friends on social media. Unfortunately, less than a quarter (21.5%) of these students indicated they had the ability to make decisions regarding the trustworthiness of a site. Less than fifty (18.7%) of students have knowledge of the different types of licenses that apply to online content with nearly half (47.3%) indicating no knowledge on how to change their privacy setting online. Whose responsibility is it to monitor and control what young people do on digital platforms? This paper explores how children are affected, protected, or harmed using technology in their quest for digital literacy. The policy implications are discussed.

Katrin Kannukene:

‘Who guards students’ data?: data specialists and Estonian educational data’

Who guards students’ data?: data specialists and Estonian educational data. Since 2004, (digital) educational data in Estonia are stored in various systems, e.g. central educational database (EHIS). Appears that students’ data, including personal and sensitive data in national information systems are quite detailed. There are opportunities to monitor each student over time, implement very complicated and diverse analyzes and make data-based decisions. Problem is that the processing of rich datasets may lead to stigmatisation, discrimination and exclusion (Berendt, Littlejohn, and Blakemore 2020). Concerning the children futures, this aspect cannot be overlooked. Behind data-based decisions are data analysts, who, apart from technological skills, are expected to think critically, be able to make connections and see the so-called big picture (Masso, Tiidenberg, and Siibak 2020). Also play data analysts a significant role to ensure data justice – “fairness in the way people are made visible, represented and treated as a result of their production of digital data” (Taylor 2017, 1). The ongoing study aims to how Estonia educational data specialists may influence data-based decision making. Semi-structured interviews are conducted with data specialists working with students’ data. The main questions were: What kind of decisions are based on students’ digital data? How is data specialist work related to data-based decisions? How can specialist ensure data justice besides right decisions? Preliminary results indicate that the work, skills, and knowledge of data specialists may play a significant role in data-based decisions. The good and bad ones.

Lonneke van der Velden:

‘Data Justice in the Classroom’

Central in this presentation is data justice in the context of education. Academic scholarship and civil society groups have highlighted the impact of datafication and surveillance on communities that have historically suffered from injustices. Against that background, the notion of ‘data justice’ (eg. Dencik; Taylor) aims to rethink social justice (struggles) in the context of the ongoing datafication of life. Also children are increasingly datafied. In educational programmes, children use apps and educational software for personalized learning. They are continuously monitored, and institutions make use of corporate software. The COVID-19 outbreak has stimulated the use of digital technologies in educational settings even further across the globe. This evolving technological landscape calls for a better understanding of what data justice could mean for children, especially in the context of education, assessment and educational perspectives. The aim of the paper is to contribute to debates on social justice and education in relation to datafication, by: 1) bridging scholarly work on data justice, children’s rights and education; 2) describing how global developments play an important role (eg. the way large tech multinationals transform educational cultures), and 3) opening a discussion on how to intervene in this landscape in a way that takes into account children's voices.

Sava Saheli Singh and Lesley Marshall:

‘#tresdancing: Speculating Surveillance in Educational Technology'

The COVID-19 pandemic has highlighted the many ways our systems are complicated and complex, making them susceptible to failure as it tests the limits of their capabilities. At the same time, these failures and the pandemic itself have provided the perfect opportunity to increase surveillance through already ubiquitous platforms and technologies. The sudden shift from in-person to online classes made educational technology the perfect setting for corporate entities to capitalize on the real need for rapid technological solutions to deal with remote learning and teaching. They did so by increasing invasive surveillance in the name of supporting educational institutions and maintaining academic integrity through problematic online proctoring software. #tresdancing, the fourth film in the Screening Surveillance series, speculates the effects of escalating surveillance and control through educational technology. In this near future fiction narrative, a young person has little choice but to use invasive augmented reality glasses as they are forced to ramp up their engagement with a new, experimental technology in order to make up for a failing grade. Using the film as a prompt and an example, we will highlight the harms this kind of insidious surveillance can cause, discuss how speculative methods can highlight these harms, and explore the practical challenges and advantages of creative and collaborative knowledge translation projects.

Education (3)

Moderator: Anouk Mols

Sidra Sheikh, Allison Gilmour and Alexis Stolberg:

'Investigating Advanced School Surveillance Technologies and Disproportionality: A Systematic Review'

A history of disparate discipline impacts on minoritized students has prompted North American school leaders to adopt inclusionary over exclusionary discipline approaches, while simultaneously investing in surveillance technology to create more secure schools. This paper examines the present literature on advanced school surveillance technology and its association with differential effects for K-12 students. We defined advanced school surveillance technology as security devices with the power to execute dataveillance (e.g., cameras, internet monitoring platforms, etc.). We identified 31 studies using both quantitative and qualitative designs that fit our inclusion criteria. The results of these studies suggested the concentrated presence of this technology in schools that largely serve poor and minoritized students, as well as an adverse association between surveillance technology and school climate. However, few studies examined the disparate impact of surveillance technology on minoritized students to sufficiently conclude if the technology equitably produces safer or more inclusive schools. We observe this as a limitation of the research and offer suggestions for future directions. The current literature fails to keep up with technology now in circulation in schools, leaving schools to make acquisitions decisions based on limited independent empirical evidence on the effectiveness or potentially inequitable risks of advanced surveillance.

Lindsay Weinberg:

‘Mental Health and the Quantified Student'

This paper examines universities’ adoption of “WellTrack”—a self-tracking mobile phone application modeled on cognitive behavioral therapy techniques—as a solution to the increase in the prevalence and severity of mental health conditions on college campuses. While there has been a great deal of critical scholarship on self-tracking within surveillance studies, less scholarly attention has been given to the use of self-tracking applications for student wellness. Drawing from a feminist materialist perspective that understands discourse and the material word as co-produced, this paper argues that the app’s design, marketing, and reception are deeply intertwined with the political rationality of neoliberalism, which centers self-responsibility and the market economy. The app encourages students to voluntarily adapt to the university’s demands for efficiency and wellness, and to the software application’s demands for interactivity, though continuous mood, thought, and behavioral self-management. Public universities are also deploying WellTrack to make their campuses “smarter"—optimized for efficiency and cost-effectiveness using information technology—under the political and economic conditions of austerity. Students are encouraged to strive towards a vision of student wellness that precludes an analysis of the structural and systemic conditions that contribute to poor student mental health, which would necessarily include an institutional critique of the university itself.

Pratik Nyaupane and Jessica Ramos:

‘The University of Surveillance: Community suppression under the guise of safety and security'

This paper explores how criminalized activities prompt surveillance within the university campus boundaries. With technological approaches adopted as solutions to systemic issues, researchers examine how the university employs surveillance mechanisms in response to incidents of violence. The university, as an institution, aims to serve as a social impetus to improve society through education. However, it upholds and perpetuates practices of white supremacy, capitalism, and colonialism, situated within or nearby existing communities, often working-class populations and communities of color. Thus, the university not only acts as a force of oppression via hyper- surveillance but embodies other suppressive practices such as displacement, economic inequality, and social injustice. Community members who may not be affiliated with the university do not possess the agency to consent to be policed by the university. Yet, they are subject to surveillance tactics by the campus police force. Grounded in the concept of racializing surveillance as explored by Simone Browne, this study focuses on understanding how the university utilizes surveillance technology in conjunction with its institutionalized police department under the guise of security and safety situated within the campus communities.

Valerie Steeves, Jacquelyn Burkell and Priscilla Regan:

‘Policy and Ethical Implications of Inferences in Education, Elections and Entertainment’

The increasing use of algorithms in decision-making has raised a number of policy issues, most particularly in terms of the possibility of decisions being based on inferences that are discriminatory, inaccurate, or unfair in other ways. Policy solutions are generally framed in terms of providing transparency and accountability. The paper will examine the (in)ability of existing data protection frameworks (in the EU, Canada and the US) to protect people from (highly accurate and revealing) inferences made from deep data analytics that use non-PII. The paper will also map other possible correctives (including data rights/human rights). This paper will specifically explore how inferences based on algorithms and artificial intelligence (AI) become issues in three different contexts: education, especially at the K-12 level; elections, as relates to targeting and tailoring of political messages to particular individuals or groups; and entertainment, particularly the Internet of Toys (Barbie). All three areas affect young people in critically important ways, both in terms of the amount and type of data collected and also in terms of the persistent effects of the data and subsequent decisions.

Housing

Moderator: Cate Hopkins

Rodrigo Agueda:

'Struggle for surveillance in a residential condominium complex'

This paper investigates the continuous search for security inside the self-sufficient condominiums of Barra da Tijuca, in Rio de Janeiro. From a newspaper archive research on the condominium's early propagandas to the current discussions and assemblies of its residents, the aim is to explore how the promises and narratives of surveillance shape the recent urban expansion on the city and the real estate market. Focusing on the implementation of a major surveillance infrastructure project in one of the main condominiums of the neighborhood, this paper takes an urban infrastructure perspective to explore urban development and the surveillance market.
Barra da Tijuca is a neighborhood in the hinterlands of the city built in the 1970s, designed to hold "urban complexes" - multi-function self-sufficient gated communities - that would seclude urban spaces from the rising violence in the city. From the early propaganda of those "city-condominiums" to recent assemblies half a century later, the promises and demands focus on two major aspects: infrastructure and security. The implementation of a large-scale high-tech surveillance infrastructure and the politics around it shows the fluxes and agencies that take place and shape promises and demands of urban life for the upper classes.

Gregory Donovan:

'Toward Qualitative Communities: Centering the Settlement House in 'Smart' Urban Design'

This paper explores how smart urban design shapes everyday life on Manhattan's West Side and considers how the industrial-era settlement house might be reformatted so as to intervene in this shaping on behalf of dispossessed communities. An ongoing educational ethnography of an undergraduate community-engaged learning course, entitled Designing Smart Cities for Social Justice, is drawn on to unpack who gets to know and belong, and how, in a region of NYC previously redesigned by Robert Moses and presently undergoing urban smartification. Like the course, this paper engages with two urban developments: the Amsterdam Houses public housing development and the Hudson Yards private development. While Hudson Yards is sold as high-end high-rises infused with proprietary platforms and algorithms that promise a "quantitative community" for mostly White occupants, the predominantly Black and Hispanic residents of Amsterdam Houses are quantified in a different way though policing and surveillance alongside increasing threats of displacement. Extrapolating from field notes, city data, and six years of participatory work with students at a settlement house attached to the Amsterdam Houses, this paper situates the multi-service neighborhood center as both a space for techno-social reproduction and a potent site for platform cooperativism.

Aleksandra Binicewicz:

'Tech Surveillance and Housing in San Francisco Bay Area: on "Landlord Tech" by The Anti-Eviction Mapping Project'

The aim of the paper is to investigate on the relation between tech surveillance and real estate market management in San Francisco Bay Area in the (post)pandemic context. In order to do so, I would like to focus on "Landlord Tech" counter-cartography project lead by The Anti-Eviction Mapping Project (AEMP). The AEMP uses digital maps together with tenants narratives to visualize how technology is tied up in gentrification processes in the U.S. By the interaction with the AEMP data is possible to understand the broader context in which smartlocks, facial recognition systems collecting biometric data, virtual doorman and other "home surveillance" devices are used by the landlords. The goal of the AEMP is not only to present troubling data, but also to create artistic counter-narratives and build an offline movement in the name of housing and social justice. In the paper I want to examine maptivism as a social practice situated at the crossroads of art, research, and activism. Furthermore, I want to ask about the impact of counter-cartography projects on the local communities in Bay Area.

Public Health & COVID-19 (1)
Moderator: Dean Wilson

Adam Henschke and Bart Anthony Kamphors:

'Public Health Measures and the Rise of Incidental Surveillance: Considerations about Private Power and Oversight'

The public health measures implemented in response to the SARS-CoV-2 pandemic have resulted in a substantially increased shared reliance on private infrastructure and digital services in areas such as healthcare, education, retail and the workplace. This development has (i) granted a number of private actors significant (informational) power, and (ii) given rise to a range of digital surveillance practices incidental to the pandemic itself. In this paper, we reflect on these consequences and observe that, even though the additional surveillance appears to be generally socially accepted as an inevitable consequence of the pandemic, part and parcel of a larger conglomeration of emergency compromises, they are not directly justified by appeals to solidarity and public health in the same way that the instigating public health measures are. Based on this observation, and given the increased reliance on private actors for maintaining the digital space, we argue that governments have a duty to (i) determine the extent to which the collateral data disclosure and activity monitoring is justified in the context of this pandemic and other future public health emergencies, and (ii) regulate and provide oversight over these practices on par with governmental essential services that engage in surveillance activities.

Amir Cahane:

'Will the purpose creep creep further? On Israel's turn to counterterrorism measures during the pandemic'

Israel's repurposing of its secret service surveillance measures for contact tracing purposes during the coronavirus outbreak is a blatant example of purpose creep, where invasive privacy infringing technologies are used for purposes other than those which originally may have justified them. In the aftermath of 9-11, for example, the FBI reutilized counterterrorism measures for law enforcement purposes. This paper first outlines the gradual – creeping - dynamic by which Israel Security Agency (also known as ISA, Shin bet or Shabak) was authorized to repurpose its vast database of communications metadata (the 'Tool') for the civilian purposes of disease control: from unauthorized use through emergency regulations to statutory law. This dynamic was revisited albeit in a condensed manner upon the emergence of the Omicron variant. Within a broader context, these coronavirus related instances of purpose creep may be a part of a more general trend, in which authorities seek to employ surveillance measures which are already contested when used for national security purposes, such as facial recognition systems. A close reading of the Israeli Court of Justice rulings regarding the use of the 'Tool' for contact tracing purposes may provide for a better understanding whether this kind of purpose creep was limited to the unique circumstances of pandemic.

Michael Birnhack:

'Urgent Surveillance: The Securitization of a Civil Crisis in Israel'

Contact tracing is an important tool to manage pandemics, in order to break the chain of contagion as early as possible. Tracing is conducted by specially trained epidemiological investigators, or by using designated technologies, typically based on data location and people's proximity collected from portable devices such as "smart phones." While various democratic countries applied voluntary technologies during Covid-19, Israel has deployed both a voluntary application, and, simultaneously, a universal, non-voluntary and non-transparent tracing system, operated by the Shin Bet, the general security service (GSS). The Supreme Court reviewed the GSS surveillance three times, limited it to some extent, but overall, approved it. This paper traces the (Israeli) use of security-based measures for managing a civil crisis, by focusing on the temporal dimension. I identify three separate but inter-related such dimensions and their mismatch: "virus time", governmental time, and legal time. The analysis is based on a close reading of the three judicial opinions, contextualized within surveillance studies and privacy law. The analysis highlights how an urgency framing facilitated a security-based surveillance, despite its questionable efficiency and its unprecedented privacy and democratic implications.

Public Health & COVID-19 (2)
Moderator: Gregory Donovan

Bruno Bioni, Daniela Eilberg, Pedro Saliba, Gabriela Vergili and Mariana Rielli:

‘COVID-19’s legacy in the acquisition of technologies by the Brazilian Government in 2020’

As the pandemic erupted and developed, hundreds of data-based technologies were employed to fight COVID-19 in Brazil, with different purposes and faulty outcomes. Online applications, cameras equipped with multiple functions and data banks were acquired and used in all parts of the national territory to provide information and telemedicine, as well as monitor isolation rates, flows of people and face mask usage, etc. The research that gave rise to this paper was based on a total of 799 FOIA requests that, complemented with other sources of information, helped identify and map out the acquisition and implementation of these technologies by the Brazilian government, at all levels, in 2020. The research identified 253 cases and the results present a thorough overview of technologies and their main functionalities, locations and scope of application, players involved in the arrangements with the public sector and other elements. A general lack of transparency and the potential for surveillance were prominents results of the research, a large empirical study that highlights the relations between public and private sector in the adoption and provision of such solutions, as well as particular data flows and structural problems of data-driven public policies, such as lack of transparency and coordination.

Niva Elkin-Koren and Mickey Zar:

‘Misguided Hopes: The Unintended Consequences of Contact Tracing Technologies’

At an early stage of the outbreak of Covid-19, the state of Israel has taken simultaneously two different approaches for assisting human epidemiological investigations: a voluntary user-friendly civilian technology, combined with a mandatory state surveillance system. The first consisted on one of the most benevolent technological designs, which reflected commitment to values such as user’s privacy and public oversight. The second consisted on one of the most malevolent technological designs: surveillance measures run by the government’s least transparent and less accountable bodies, the General Security Service (GSS). While in the first case it was expected that users will flock the app store, the use of the GSS tools over a civilian population was perceived as a possible harbinger of “the end of democracy”. However, while the civil app appraised qualities have not convinced users, the GSS was gradually disarmed of its unbounded intrusive powers through a mixture of institutional efforts. The paper argues that the prevailing approach, which place tremendous weight on the power of technology to solve societal problems by embedding social values is flawed. Rather, design choices interface with institutional design, thus making technological outcomes and social implications dependent upon a much more nuanced ecosystem of various actors.

David Lyon:

‘Surveillance capitalism meets the pandemic: Surveillance challenges to the ‘social contract’

Data-dependent ‘solutions’ to problems posed by the COVID-19 pandemic have been proliferating, globally, since early 2020. These range from digital contact-tracing to the establishment of large-scale data platforms for modelling and monitoring the progress of the virus, with many apps, devices and systems in between. Together, they contribute to the largest surveillance surge since 9/11 and come with similar ‘emergency conditions’ rationales that demand public compliance with government requirements. These are widely proposed as temporary challenges to some ‘social contract,’ but it is increasingly unclear who are the participants in this ‘agreement,’ especially as public-private partnerships have multiplied during the pandemic. Familiar concepts, such as ‘function creep,’ ‘shock doctrine,’ and ‘social sorting’ each require rethinking for this circumstance. The global COVID-19 pandemic offers opportunities for recalibrating some taken-for-granted ways of understanding the relationships between surveillance operations and experiences.

Joana Fonseca:

‘*Eggers' post-pandemic technodystopian speculations on surveillance'*

One of the fascinant aspects of surveillance as a subject of speculative fiction is the aesthetical possibility of a material description of surveillance devices and apparatuses, their focus and consequences. This is exposure of surveillance itself, that usually carries an emergency warning dimension, the information in the form of the worst-case scenario, which is also a form of performing 'artveillance', as Brighenti describes it. The creation and consumption of artveillance can be an act of aesthetic counter-surveillance. Dave Eggers' "The Circle", follows Mae in her enroling as a worker in this big company, similar to Google or Amazon, and the consequent loss of privacy plus the imposition to create and promote transparency. Eggers captures the current environment not only of corporative surveillance but also of the social imposition of online participation, of an investment and development of an online self. On a totally offline trip to the bookstore, I came across "The Circle"'s sequel, The Every, that goes deeper on the inadequacy of the human-machine, a feeling that grows in a post-pandemic, mostly digitally mediated and ultra-monitorized super-tech-era. "The Every" mirrors this culture of surveillance, the self and outro control that sneaks between these leaky containers.

Social Relations and Capitalism (1)

Moderator: Alessandro Caliandro

Courtney Hagen Ford:

‘Family Surveillance Products - what are they and why do they matter?’

By now, intimate surveillance (Leaver 2015, 2017) is well-know and established, but the tools through which it is enacted in everyday settings less so. This paper will explore the emerging category of family surveillance products (apps, products, and services that parents can use to monitor their own children) by defining it, explaining its relevance to surveillance studies, and demonstrating how contemporary UK families use these products in their everyday lives. This paper, comprised of data from the author’s PhD thesis, provides an original contribution to the field by taking into account the perspectives of both parents and children in the same work. Diverse members of sixteen different families were invited to participate in semi-structured interviews, with the resulting data analysed through the precepts of grounded theory. Insights into gender, risk, consumption, contemporary parenting, and contemporary childhood will be offered.

Susanne Oechsner:

‘“No camera”. The ambivalent surveillance potential of sensor-based AAL spaces’

In recent years, demographic aging has been established as a pressing socioeconomic problem for European societies and Active and Assisted Living (AAL) technologies as solution to support older people’s ageing in place. This paper draws on qualitative interviews with researchers/developers in Austrian AAL projects to explore experimental project spaces in which sensor-based AAL technologies are being developed and to investigate ambivalences in dealing with the associated surveillance potential. On one hand, project researchers/developers strongly subscribe to AAL’s potential of better seeing informationalized bodies (van der Ploeg 2012), which promises timely interventions in case of emergency and proactive strategies based on pattern recognition, prediction and control (Conrad 2009). On the other hand, they continuously manage and downplay potential associations with well-known tropes of surveillance that could endanger the project itself and experimental subjects’ participation in it. Aside from discursive closure mechanisms, the understanding of a limited experimental project space may cause the surveillance issues to subside. Yet, I will argue that projectified experimental spaces may have the effect of transforming experimental subjects into future users, retaining and normalizing the spatiotemporal surveillance of subjects/bodies.

Anders Albrechtslund, Astrid Meyer and Stinne Aaløkke Ballegaard:

‘Negotiating dementia care: How surveillance technologies twist and intertwine with safety, dignity and privacy’

The implicit ambiguity of surveillance as both control and care has been a key theoretical issue in social science research on surveillance practices and technologies since the foundational work of Michel Foucault. This issue also reflects a prevalent socio-technical perspective in which a central factor in considering technology’s effects on society and relationships is always contextual and situational. This paper will explore the ambiguities of surveillance in light of an ongoing research project focusing on the use of technologies for care and control in healthcare of elderly with dementia. Through this case study, we will emphasize how virtual (and sometimes actual) struggles lie in the ambiguities between care and control brought about by surveillance technologies. In doing so, this research project offers insights into how surveillance technologies twist and intertwine with the notions of safety, dignity and privacy that govern caring for a vulnerable group such as elderly with dementia. In the article, we examine how relatives and caregivers struggle with reconciling the use of surveillance technologies with the maintenance of a trustful and considerate relationship with those they look after.

Dario Pizzul, Guido Anselmi and Alessandro Caliandro:

'A systematic literature review of surveillance capitalism'

Although surveillance capitalism - as intended by Shoshana Zuboff - is an emerging topic, it already attracted the attention of many scholars from different fields within social sciences. Therefore, in this contribution we propose a systematic literature review of the topic of surveillance capitalism. Specifically, we developed a systematic literature review on a pool of 161 academic articles automatically extracted (through a Python script) from ad hoc scientific sources (e.g., Scopus), which we processed with computational techniques of text analysis (e.g., co-word analysis, topic modelling, TF-IDF). Also, a close reading of a sample of 30 articles was conducted. Results show that the topic of surveillance capitalism is composed by six main sub-topics: marketing & social control, big data & datafication, platforms & platformization, data privacy & protection, culture of surveillance, AI. We argue that all these key sub-topics need to be addressed attentively (or at least taken into consideration) when dealing with academic research and/or writing on surveillance capitalism, also paying attention on how each dimension inform and co-construct each other.

Social Relations (2)

Moderator: Adam Molnar

Kara Brisson-Boivin and Samantha McAleese:

'"It gets kinda creepy sometimes": Young Canadians share concerns and solutions about online privacy and surveillance'

This paper draws from three qualitative research projects conducted between 2019 and 2021 – one on online resilience, one on privacy and consent, and the other on algorithms and AI. All projects involved conducting focus groups with youth ages 11-17 from across Canada, asking them about various aspects of being and interacting in the online world. Two focus groups incorporated interactive components to facilitate real-time learning and creative collaboration to bolster discussions. One narrative that runs through each of these projects is that of surveillance. Youth from across Canada shared their concerns about data collection and sharing, machine learning, recommendation algorithms, corporate surveillance, and the potential future consequences of sharing content online. We will summarize these concerns and observations in addition to the many solutions and recommendations that emerged from these conversations. Results from all three qualitative studies are not only a call to action for educators, policymakers, regulators, and online platforms – but also a reminder that young people are experts in their own lives and come to the table with solutions for adult-made problems.

Ozge Girgin:

'The Disjuncture: Perception of Smartphone Surveillance'

Smartphones, mobile apps and social media have a crucial role within the contemporary culture of surveillance. Looking at meanings, practices and attitudes of surveillance subjects concerning these technologies can help us understand surveillance values, norms and expectations from their perspective. This can allow us to explain how surveillance functions within the routines of everyday life. The presentation will share the findings of one-to-one and focus group interviews conducted with young adults from various social locations in Turkey in relation to their understanding of vertical surveillance practices through these technologies. My findings reveal the disjuncture between the data that young adults consider important and the data in which corporations are interested. The presentation argues that this disjuncture can be partially explained in a Turkish context by dominant persistent surveillance imaginaries in Turkey arising from contextual interplay of cultural, social, and political context. The presentation also asserts that the uncertainties that people have with regards to their data flows, and the perceived proximity of consequences of surveillance needs to be taken into consideration when attending to surveillance subjects' meanings. Users have a contextual understanding of their data flows. Moreover, the emphasis on data security, the unknowns that users cannot envision about data flows, the emotional ties formed with platforms, conceptualization of data sharing as 'how the system works, and problematization of surveillance mostly in individual terms contribute to this disjuncture and users' understanding of platforms as confidants.

Liisa A. Mäkinen:

'Privacy in the context of smartphones – Empirical examination of young peoples' perceptions of data gathered to and through their phones'

Young people spend most of their waking hours on their phones and online: in Finland 99% of people aged 16 to 24 use the Internet on a daily basis and 98% use it with their smartphone. Previous research recognizes internet as complex surroundings for young people as it enables them to explore their identities but at the same time subjects them to vast amounts of surveillance. Smartphone adds a layer to online data collection as it also enables location tracking, can utilize biometric data, and is often used as a camera device. This research builds on empirical data gathered in Finland focusing on young peoples' perceptions on data gathered on them by their smartphone and its apps. The data collection in this research utilized a mixed-methods approach combining concept mapping and Q-sorting approaches to in-depth interviews of research participants. Altogether forty people aged 13-19 participated. This presentation focuses on examining which data young people consider most private to them and why, to whom they want to share that data, and from whom they would prefer to hide it. The aim of this research is to analyze how young people understand, manage, and value their privacy.

Anouk Mols:

“My friends’ parents are probably a lot less strict”: Negotiations around family surveillance in interconnected families'

The embeddedness of digital technologies in everyday family life creates endless communication and entertainment opportunities and allows parents to monitor the educational progress, media use, and whereabouts of their children. Whereas not all families are interconnected to the same degree, many parents and care-takers struggle with finding a balance between control, care, freedom, and digital well-being. This study explores how families negotiate tensions around power, control, and privacy that go hand in hand with family surveillance. Family surveillance is defined as a lateral process of keeping track of the digital and non-digital activities and associations of family members. The research focuses on nine families in the Netherlands with different set-ups and cultural backgrounds; interviews were conducted with eleven parents and eleven early adolescents. Parents discuss how they approach screen time restrictions, location tracking, social media monitoring, and student tracking systems. Their children reflect on how they experience such surveillance and describe responses ranging from acceptance to active resistance. Drawing on these findings, it becomes clear that family surveillance is embedded in broader constellations of media and communication practices and sometimes occurs in reciprocal ways. Open conversations about technology are advised to foster surveillance awareness, and privacy and cybersecurity resilience.

Carsten Ochs:

‘Deep Targeting'

For two decades now a whole industry is busy bringing data-based targeting techniques to perfection (Zuboff 2019). Legal, philosophy, and ethics scholars’ have responded to this in recent years by developing novel conceptual and normative ways to deal with behavioral control (Taylor et al. 2016; Susser et al. 2019; Mühlhoff 2021). Karen Yeung (2016), who has developed the influential notion of “hypernudging”, has been most straightforward in pointing to the necessity of a genuinely sociological treatment of these issues. The proposed paper is thus addressed to this task, by offering a synoptic analysis of contemporary targeting techniques from a decidedly societal perspective. It does so, by 1) providing a pluralistic pragmatist conception of experience (experiential contingency) as the subject of protection when it comes to targeting; by 2) specifying the societal fabric being targeted by behavioral control with the aid of systems theory’s fourfold distinction between social/factual/temporal/spatial dimensions of society; and by 3) showing how contemporary targeting in fact operates in all these dimensions, thus interfering in the overall fabric of society. This is what I call “deep targeting”, an intensification of surveillance that might perpetuate the one occurring in the transition from Ancien Régime to nation state (Giddens 1987).

Subjectivities and Workplaces

Moderator: Ciara Bracken-Roche

Camilla Cannon:

‘(Un)Governable Genders: Possibility, Potentiality, and State Gender Identity'

In recent years, the United States has seen a number of state legislative and policy changes which allow for transgender individuals to request gender marker changes on their birth certificates. Additionally, some states have begun to offer third, non-binary gender options for official documents like driver’s licenses. While these changes undoubtedly materially improve their lives of many trans people, I join a number of trans scholars who are concerned about the surveillance and administrative ramifications of these changes. In this paper, I argue that seemingly trans-inclusive state “reforms” of gender marker policies aim to render trans and gender non-normative individuals as optimally legible and governable subjects while simultaneously affirming the authority and infallibility of the state. I situate my work within broader surveillance studies conversations regarding the rise of risk management thinking in private and public industry, proposing that the institutionalization of gender marker changes and third-gender options seeks to nullify the destabilizing potentiality of (trans)genders while reinforcing the individual’s affective and logistical connection to the state.

Cate Hopkins:

‘Solidarity Under Scrutiny: Collective Action in a Digitised Workplace'

The surveillant capacity of workplace technologies demonstrate how human experiences can be reduced to numerical data that evaluates worker performance against targets and expectations (Moore 2018). Unlike industrial capitalism, which profits from the exploitation of labour and natural resources, surveillance capitalism exploits information and analytics for profit (Zuboff 2014). The trade union movement has historically resisted the worst excesses of industrial capitalism (Hobsbawm 1968), which have been largely visibly and collectively shared. Our digital lives are more individualised, and experiences of oppression are not necessarily mutually shared but linked to our identities as gendered, racialised, embodied persons (Dubrovsky 2014). Trade unions have acknowledged some of the challenges presented by the digitised workplace (TUC 2018), but cohesive responses are still in their infancy. This paper draws on interviews conducted with trade union activists from the public sector to explore challenges presented by the digitised workplace. It explores their understandings of workplace surveillance and its capacity to shape trade union organising strategy, and asks how workers can build solidarity around issues that are so often highly individualised. How do they define ‘surveillance?’ How do they encounter it in the public sector in the UK? How can solidarity be built around this issue?

Michael Zimmer and Jessica Vitak:

‘Privacy and Power in a Pandemic: Examining Remote Workplace Surveillance Practices During COVID-19'

The COVID-19 pandemic has created new opportunities–and tensions–around workplace surveillance. In the initial months of the pandemic, office workers suddenly needed to coordinate work and meetings remotely, while employers deployed advanced tools to monitor employee productivity. While some forms of monitoring are appropriate in these circumstances, others raise questions about privacy and power, especially when the boundaries between work and home are blurred. Further, questions remain whether such pervasive surveillance practices will continue after pandemic-fueled restrictions ease. We present results from a survey of 650 American office workers who shifted to remote work for at least part of the pandemic. We employed factorial vignettes, a survey method that presents respondents with a series of scenarios–in this case about possible employer surveillance practices–to unpack specific contextual factors that might be seen as more or less problematic by workers. Utilizing Nissenbaum's framework of privacy as contextual integrity, our findings provide insights into workers' perceptions of current workplace monitoring practices and, more importantly, their concerns regarding the potential uses of workplace monitoring technology as they return to "normal" working environments. We also raise new questions about how reductions in privacy and independence at work may negatively influence worker productivity, satisfaction, and well-being.

PANEL: Surveillance & Subjecthood: Gender, Race, & Class in the Constitution of Data Subject
Panelists:

Laura Carter
Jens T. Theilen
Aisha P.L. Kadiri
Felix Bieker

Questions of subjectivity and subjecthood have been essential to surveillance studies since their inception. Increasingly, scholars are investigating how surveillance (re)produces differentiated forms of subjecthood along the lines of gender, race, and class: the constitution of Blackness through the white gaze, the deepening of gendered capitalist subjectivities through digital reproductive labour, the perpetuation of (cis)gender norms and racialised logics through airport scanners, and much more. State regulation of surveillance also generates subjecthood through the concept of a "data subject". We aim to extend and deepen these discussions by bringing three accounts of surveillance and subjecthood with a focus on gender, race, and class into conversation. We thus hope to explore processes of surveillance, data processing, state regulation, and resistance across a variety of contexts and from different perspectives.

Jens T. Theilen will discuss the surveillance of trans and gender-nonconforming persons with a focus on the operation of gender norms and processes of racialisation. They argue that approaching the legal regulation of gender against this backdrop opens up new avenues for considering how trans subjectivities are shaped, with both surveillance and legal regulation imposing legibility for cis persons ("cislation") as a core requirement.

Laura Carter will discuss the ways in which the welfare benefits system in the UK increasingly uses data-based surveillance to determine who is "deserving" of support. She argues that this increased use deepens the (already-significant) extent to which welfare claimants are monitored

for compliance with gender stereotypes, risking a vicious cycle in which claimants, fearing discrimination and denial of benefits, are increasingly coerced into demonstrating this compliance.
Aisha P.L. Kadiri will offer an account of what she terms the "autopoietic data subject", investigating which subject ontologies are formed within and through data colonialism. Both the global digital economy operating on surveillance and extraction as well as efforts to guardrail it via privacy and data protection rely on the concept of the data subject. Kadiri argues that this builds on contextual concepts of personhood and humanness, which are upheld through a self-sustaining, autopoietic logic.

STREAM 8: TECHNOLOGIES

Algorithms
Moderator: Michael Zimmer

Dominika Iwan:

'Mitigating discriminatory impacts of surveillance algorithmic decision-making systems through data governance'

The paper explores discriminatory algorithmic decision-making (ADM) at the data level and argues that mass surveillance ADM systems affect all human beings but not equally so, and the most affected are persons belonging to vulnerable groups. Consequently, there is a need to explore which data governance model would contribute more to prevent or mitigate disparate treatment or impact of surveillance ADM systems. The paper consists of three parts. First, it describes the main reasons for discriminatory ADM systems, namely a human, data, and an ADM system. Secondly, the paper focuses on how data gathered or collected by surveillance ADM systems result in discriminatory outputs. Eventually, data governance models, as tools for addressing the collective dimension of surveillance ADM systems, are evaluated in order to prevent discrimination of these systems. The contemporary data governance models grant individuals hardly any measure of control over their personal data. Therefore, the only available consent-based approach towards data privacy enables the individual to either consent or decline to the conditions of delivering a product or service. The new data governance models, such as data trusts or information fiduciaries, encourage transparency and contribute to detecting data bias while sharing data, and consequently mitigate discriminatory algorithms.

Thomas Behrndt:

'Coming to Terms with Algorithmic Surveillance'

We are now living in a world which is defined by ubiquitous surveillance, produced and sustained by mass data-collection and analysis, operating often remotely through embedded networks. Surveillance can be understood as social sorting, referring to the specific arrangements "coded to categorize personal data such that people thus classified may be treated differently" (Lyon 2007, 162). The analysis (or sorting) of this data is an increasingly automated process conducted by networked systems utilizing advanced algorithms. While not exclusively, most contemporary surveillance practices have become algorithmic in some sense of the word. The term algorithmic surveillance is often used literally, referring to surveillance utilizing algorithms; more specifically, however, it also denotes "surveillance technologies that make use of computer systems to provide more than the raw data observed (Introna and Wood 2004)." I am arguing that to understand contemporary surveillance practices, we must come to terms with the role played by algorithms and the implications they have as actors in a complex socio-technical space. Thus, it is important to understand what is specific or different about the algorithmic aspects of contemporary surveillance in advanced societies. The paper is divided into four parts. The first two parts, will provide both a historic as well as current account on debates and understandings of algorithms. Part three, develops the argument of understanding algorithms as an epistemological frame, exemplified by a discussion of William Uricchio's notion of the algorithmic turn. The fourth part, returns the discussion to question of (algorithmic) surveillance.

Pete Fussey:

'Reconsidering rights and ethics in the era of digital policing'

Recent years have seen a growing digitalisation of law enforcement practices and step change across a range of surveillance capabilities. Companioning this growth has been an intensification of discussions concerning the agility and adaptability of regulatory and legislative frameworks to govern such uses. This paper draws on first-hand empirical fieldwork of embedded digital policy practices, including ethnographic research of active facial recognition surveillance operations in the UK and digitally-assisted patrolling in the US, to analyse how complex operational milieus yield a range of unanticipated digital practices that, in turn, assert rights-based implications. The paper also draws from author engagement with national surveillance oversight roles and participation in surveillance-related litigation processes (e.g. Bridges 2/England & Wales Court of Appeal) to assess how these rights concerns arising from emergent digital surveillance practices remain unanticipated and unaddressed in extant regulatory frameworks.

Artificial Intelligence

Moderator: Jorge Pereira Campos

Pinelopi Troullinou:

'Mapping the controversy ecosystems of AI tools in the security domain'

There is an increasing reliance on innovative technological measures to predict, investigate, and combat crime promising more effective citizen and border protection, safety, and security. European Union has been evolved into a dominant defense technological power (Csernatoni, 2021). To this end, European Union invests over €270 million in artificial intelligence and security research (European Commission, 2021). However, the developments and applications of AI technologies especially employed by law enforcement agencies (LEAs) raise great controversies in the view of an Orwellian surveillance state. Publicity over the extensive use of personal data in the name of security such as Snowden's revelations but also China's Social Credit system have increased public awareness and sensitivity over privacy. Concerns over the "surveillance-industrial complex" (ACLU, 2004) have been brought into the public discourse following scandals such as Cambridge Analytica data.
This paper will provide a map of AI in policing innovation ecosystem identifying who and about what is shaping the concerns and potential of AI in security. The critical assessment of this map will expose potential gaps in the stakeholders' representation such as the exclusion or underrepresentation of vulnerable groups most affected by these developments. Furthermore, it aims to show potential limitations of the controversies reducing any debate in data protection and privacy-oriented focus. Drawing upon surveillance studies literature the critical analysis of this map contributes to the discussions about the democratisation of algorithmic surveillance (van Brakel, 2020).

Jaana Okulo:

'Machine Attention'

The paper discusses attention through its psychological and philosophical aspects in order to provide interdisciplinary understanding on how information gets constructed in current machine learning models. Attention is the key constituent of knowledge as it determines what arises as information from the perceived signals. In machines, it enables the capture of perceptual content often through linguistic mappings. Also, saliency models, even trained from human gaze patterns, seem to attend semantic objects similarly to linguistic models. Critical thinking should be directed to the limited use of the concept 'attention'. Attention is a rich philosophical term with extensive psychological research covering its main aspects. The literature shows how we don't only attend through linguistic reasoning, but attention can be directed to the dynamic nature of sensory information in a nonverbal manner. Even object detection is an elementary process for human cognition, and it enables the vast number of modern tasks targeted with machine learning, it also creates the basis for stereotyping. Attending high-level concepts lets the perceiver ignore a drastic amount of complexity.

Mike Zajko:

'AI as Automated Inequality'

This article addresses how artificial intelligence (AI) and algorithmic decision making (ADM) contribute to the reproduction of social inequality, and the relevance of surveillance to these issues. Particularly for machine learning algorithms, surveillance studies can inform our understanding of how training data is constructed, which then becomes the basis for algorithmic prediction and classification. Problems with over/underrepresentation of human categories in training data are based on differences in visibility, how some populations are more/less surveilled, or differentially targeted for data extraction. Surveillance is often presented as a solution to these problems, whether through collecting more training data about marginalized groups to equalize outcomes, or by monitoring and auditing algorithmic decisions. Marginalization is reproduced when disadvantaged populations are excluded from datasets that train algorithms to provide care and benefits (as in health care), but also when disadvantaged populations are disproportionally included in data that informs more punitive outcomes (as in policing). Finally, algorithms discriminate on the basis of underlying social inequalities, when these appear as patterns in training data (as in predictions of outcomes based on historical patterns). More or better data is not the solution for many of these problems – a critical position that surveillance studies can help to inform.

Contested Technologies

Moderator: Colin Bennett

Crofton Black

'Commercial telecom surveillance: economic and technical aspects of network access'

The deregulation of the telecom industry, while offering greater flexibility to consumers, also allowed a number of third parties to monetise vulnerabilities in the global mobile phone network for geolocation and intercept purposes. This paper will draw on my work in progress (from 2020 and ongoing) to look at the ecosystem of actors in the telecom surveillance space and the economic conditions underlying their activities. In particular, I will discuss the roles of global title leasing and mobile virtual networks, and look at how, and why, some market-disrupting innovations have benefited the surveillance industry.

Renée Ridgway

'Black Box vs. Black Bloc: Reimagining Google's surveillance capitalism through Tor's agencies of anonymity'

In 1981, Shoshana Zuboff cogently pointed out the fundamental duality made possible by the new IT tools of capture, with information technology alone having the capacity to 'automate and to informate', thereby not only imposing information but also producing information. Collected by devices 24/7, 'informal actions' of users such as search queries reflect this 'unceasing flow' of information—what was before not commensurable became 'textualised', or codified as data, with 'signals' revealing human behaviour (Zuboff 2015). With 5,6 billion requests per day, 'ubiquitous googling' (Ridgway 2021) has been grafted as a paradigm for the way users find information as they 'voluntarily provide' data in exchange for free services. Value resides not only in the primary applications of data gathering techniques but rather in the innovative, secondary purposes that were not even imagined when it was first collated (Mayer-Schöneberger & Cukier 2013). As Google becomes more

arcane about its ‘logic of accumulation’ (Zuboff 2015) and data (re)usage, the ‘searching subject’ becomes increasingly ‘unboxed’ through filtering and sorting processes of personalisation. Yet the alternatives to Google Search remain underexplored.
In this visual presentation I show results from 'Re:search - the Personalised Subject vs. the Anonymous User', which compares Google’s personalisation to anonymity searching with the Tor (The Onion Router) browser. With a ‘critical ethnography of the self’, I designed an ‘experiment in living’ (Marres 2012), gathering data on myself and imaging the results with my method, ‘data visualisation as transcription’.
Departing from Alexander Galloway’s Black Box, Black Bloc text (2011), I demonstrate how Google’s black box effects shape not only the web (Introna & Nissenbaum 2000) but organise (us)ers through their online habit of querying (Ridgway 2021), with the capturing of their IP (internet protocol) address. Instead of just ‘organising the world’s information’, advertising companies (Google) simultaneously construct 'subjectivities of search' through ‘cyberorganization’ (Parker & Cooper 2016)— where Google’s proprietary algorithms assign users into collectives of others ‘like them’ (Chun 2016; 2019).
In contrast to Google’s ‘behavioural surplus’ of user data that creates prediction products facilitated by surveillance capitalism (Zuboff 2015), tactics of resistance can provide users with obfuscation (Brunton & Nissenbaum 2015), such as Tor that hides their IP address. Other ‘black bloc’ effects range from pseudonymity or degrees of ‘unreachability’ (Nissenbaum 2015), to programming bots that imitate human interaction.
I argue that aside from its other merits in terms of circumventing surveillance by state and corporate actors, trusting Tor can be a strategy to organise political agency. As one of the few alternatives to becoming a personalised subject, not only do ‘platforms intervene’ (Gillespie 2015) but also users with various 'agencies of anonymity'.

Lucas Pereira Baumgartner:

‘Mapping the unknown: the cartographer in the Deep Web’

The "Deep Web" seems to be a place almost mythical. Supposedly, it is the place where criminals can hide and share the most nefarious content. However, putting aside all the media content, what we have are alternative networks and different methods of using the Internet. This paper focuses on the users of those networks, more specifically the Tor-network users. The goal is not to unmask these people but to map them, identifying power relations between those who want to be hidden and the surveillance structure we have today. To do so, we studied the phenomena from the Tor-network user's point of view, applying a transdisciplinary methodology: first, we conducted 12 semi-structured interviews with Tor-network users; secondly, we analyzed the interviews, searching for patterns; and finally, we analyzed all the data inspired by Jesús Martín-Barbero's cartography. The results are two maps: one exploring the relationship between the groups of Tor-network users, and the second a map that explores power relations. My argument is that Tor-network users not only fight for their right to be anonymous but also fight against the mythical "Deep/Dark Web" and the pejorative image it represents.

Sarah Young, Catherine Brooks and Jason Pridmore:

'Anticipating Quantum Surveillance'

Quantum networks are changing the visibility of information and moving us into new paths of surveillance. One particular way we can see the influence on quantum is quantum key distribution (QKD). QKD is a method of exchanging encryption keys along networks to ensure that only authorized parties get access to the information being communicated. In that regard, QKD is also a method that redefines surveillance practices in the near future and requires a reconsideration of policies relative to quantum network governance. Because surveillance is almost synonymous with ICTs in that they send, track, save, and categorize personal information (Sewell and Barker, 2007), changes in how those processes happen will impact how we view, understand, and control surveillance practices. To offer an entry point into conversations about surveillance relative to quantum-based methods, this presentation offers a technocriticism of QKD as a method or task, an analysis that can provide insight into the future of surveillance and related policy. We conclude that QKDs and their associated network structures not only change what we know about security, but they also alter conceptually what we know about surveillance and how policy shifts will likely follow if public interests are to remain in focus.

Design & Coding

Moderator: Daniel Trottier

Silvia Masiero:

'Digital Identity as Platform-Mediated Surveillance: A Study of Design Properties'

Digital identity systems can lead to surveillance. In social protection schemes, the right to assistance is subordinated to registration of biometric data, making digital identity a tool to police and profile rather than assist. Yet, the design properties of digital identity platforms find limited space in the surveillance discourse: first, enabling the construction of complements in digital identity platforms is the availability of boundary resources made accessible to third-parties. Second, thanks to generativity, third-party actors can build complements on the platforms' core using boundary resources. Based on such design properties, this paper develops the concept of platform-mediated surveillance. I use ten-year qualitative data on India's Aadhaar platform (the largest digital identity platform in the world) to illuminate how the interoperability of Aadhaar with other systems, ranging from food security to public health insurance, affords the undue surveillance of vulnerable groups, essentially leading vulnerable people into the binary condition of either registering and becoming profiled, or giving up essential benefits received from the state. Implications of this reflection are drawn for recent issues of post COVID-19 social protection and vaccine distribution, illuminating how the design properties of digital identity can exacerbate extant inequalities and ultimately reinforce the "dark side" of such platforms.

Tommy Cooke:

'Big Data Exposed: Or, How Third-Party Remote Extraction of "Raw" Satellite Signal Measurement from Smartphones is Fuelling the Demise of Location Privacy'

This paper presents "Big Data Exposed": a multidisciplinary research experiment that brings social scientists and computer scientists together to (a) demystify and (b) critique how corporations and governments extract smartphone location metadata for profiling purposes during the pandemic. Launched in the Fall of 2021 at Queen's University, the experiment involved the retrofitting of two smartphones with data tracking software. The devices were carried across three specific travel routes across Kingston, Ontario, Canada while specialized software monitored how a third party Mobile Location Analytics (MLA) corporation in The Netherlands profiled our devices' movements in real-time. This paper discusses three of the project's initial findings, which emphasis on the MLA's extraction of a single variable produced by the Global Navigation Satellite System (GNSS) receiver within smartphone. I trace empirically this variable through its usage by Google, the European Global Navigation Satellite Systems Agency and the French Space Agency to (i) develop sub-metre predictive tracking algorithms, (ii) develop anti-spoofing/location simulation by smartphone users, and (iii) to fuel the STRIKE3 global signals interference surveillance, detection, and jamming network. The paper concludes by outlining the need to radically re-think location privacy along the lines of discrete navigation satellite signals measurement extraction processes, which remain undiscussed by surveillance studies scholars.

Keren Levi-Eshkol and Rivka Ribak:

'Privacy by design and privacy by policy in GitHub README files'

Most digital products use technologies that enable the collection, analysis and transfer of a considerable amount of personal information to the cloud, where it is stored and processed. Thus much of the responsibility for the users' personal information is in the hands of the developers and the code that they author. This research adopts a materialist perspective to study developers' discourse around the privacy solutions they embed in the code. Defining GitHub as a discursive platform, we draw on a sample of almost 60,000 README files to analyze the ways in which developers present code to other developers. We find that the files promote two approaches, privacy-by-policy and privacy-by-design. We suggest that the choice of privacy protection practice is connected to the need to comply with state laws and with the technological giants' regulations.

Faces & Face Recognition Technologies

Moderator: Donya Hatami

Anthony Minnaar:

'Facial recognition and cybersurveillance in public spaces: Issues of privacy, ethics vs security'

Facial recognition technology has been in use for many years but recent technological advances, including the use of artificial intelligence analytics, has led to several concerns and issues being raised regarding its ever-spreading use by government departments (e.g., migration and border control; ports-of-entry; policing and security agencies). Furthermore, the development of more advanced facial recognition surveillance technology has created more potential risks for the misuse of personal data and the violation of human rights. For instance, the newly developed 'iBorderCtrl' test analysed incoming travelers crossing international borders while being questioned but simultaneously having facial micro-gestures (face and eye) discreetly scanned by webcams with the aim of determining whether travelers were lying about the purpose of their trip. However, while automated border control systems, for example: 'SmartGates', have been used since at least 2007 to speed up traveler entry by using facial recognition to verify traveler's identities against data stored in biometric passports, the further proliferation of CCTV smart cameras with built in facial recognition capabilities and AI analytics in cities' public spaces has heightened the fears of: a) databases being hacked; b) invasion of personal privacy, even in public spaces, and therefore unknown to those being so surveilled; and c) the use of facial recognition databases to mine other databases, for example: the use by the US Immigration and Customs Enforcement Department (ICE) between 2014 to 2017 of facial recognition data to mine state drivers licence databases to detect 'illegal immigrants'. Such data misuse of facial analysis is not only scientifically questionable but also ethically abhorrent. A case in point is the company called Clearview that for more than two years prior to 2020 surreptitiously gathered billions of photos – all available online – to create an app that searches people's faces to help identify who they are. This paper discusses and tracks several of the more recent controversies and concerns surrounding the use of facial recognition analytics in a number of settings.

Sharrona Pearl:

'Face Recognition Software and Machine Translation: Why Computers aren't people'

This paper will put the awkward and ongoing hype around super recognizers and face recognition technology and the biases therein in a long historical trajectory to explore the history of face recognition software and surveillance. I'll use computer language learning as a model for why face recognition technology will only ever be as good (or bad) as its programmers, and what that means for face recognition more broadly. We'll see how face recognition technology originally tried to mimic what people did. That didn't work. So researchers pivoted and tried to solve the problem a different way. Rather than acting as an ethical conundrum or a social mediator or a surveillance tool, face recognition technology was a problem to be solved. Researchers tried a number of approaches, and it was only with the introduction of eigenfaces in the early '90s that the thing sort of started to be possible. With one set of problems solved or at least solvable, a whole bunch of new ones emerged. The math became clearer; the ethics became a whole lot more muddy. But these two problems are not distinct. In fact, as the work of the algorithmic bias researchers show, they are in many ways the same. And that matters for the work of face recognition, and it also matters for how we conceive of the relationship between humans and machines, and humans as the redemptive technology for the shortcomings of machines. Which means – always and necessarily – that the biases of the humans get reproduced and amplified in the technologies of the machines. As this paper will trace, it has always ever been thus.

Shivangi Narayan:

'Facial Recognition and the Criminal City'

This paper wants to investigate how surveillance technologies used by the police such as the current use of facial recognition technology further solidify the perception of poor areas of the city as criminal thus limiting the opportunities of the residents of these areas culturally, socially and economically. Slums, immigrant colonies, shanty towns have long been considered as hotbeds of crime and illegal activities. These areas are generally marked as unsafe in the popular imagination. I am interested to see the ways in which communities in these spaces modify their behaviour in order to escape the extra watchful presence of the state in the form of CCTV cameras. I also want to see how these spaces evolve in terms of their interaction with other parts of the city as a result of the use of such exacerbated surveillance technologies. This paper will be based on ongoing ethnographic work in one such marked area in the North East part of Delhi which is now being heavily surveilled using facial recognition technology following deadly riots that killed a record number of people and destroyed many businesses in February 2020.

Rohan Faiyaz Khan, Sam Baranek, Georgia Reed and Catherine Stinson:

'Before and After Pseudoscience: An Empirical Challenge to Social Classification using Facial Recognition'

A number of researchers and companies claim to be able to discern social category membership (criminality, sexual orientation, political orientation, etc.) using facial recognition and AI, and suggest on that basis that these categories have a biological basis that can be detected and surveilled automatically. Critics have raised both political and methodological challenges to these claims. Here we re-implement a study that claims to be able to discover political orientation from face images posted to social media sites using LASSO regression and neural networks, and subject it to empirical challenge. We create a novel dataset consisting of pairs of pictures of 10,000 individuals where the individual is presenting themselves differently in the two pictures, drawn from searches for "before and after" images from makeovers and haircuts. The alleged political orientation detection algorithm classifies the two images of the same person differently 20% to 50% of the time, depending on method. We also retrain the algorithm to predict "before" and "after" categories on the new dataset, and achieve prediction accuracy of 60%, which is comparable to published results. These results verify the suspicion that superficial presentation differences, not biological factors, are responsible for social classifications using facial recognition.

Marnie Ritchie

'Occupied Emoting: The Black Face as Misrecognized Medium in Affective AI'

Adrian Daub (2018) recently announced “the return of the face,” more specifically, the return of physiognomy, “the attempt to interpret a person’s character by means of their face.” This essay shows how the distorted Black face acts as a medium in the historical development of the claim that universal emotion can be read from facial cues. This article closely reads the colonial affects in the influential work of Paul Ekman and his early experiments to develop a set of universal emotions. Through a consideration of Martinique psychiatrist Frantz Fanon’s Black Skin, White Masks, this essay engages Ekman’s early practices of emotional extraction as based in phobic presumptions of Black pathology. Ramon Amaro (2019) writes, “[I]t is apparent that the black technical object is always-already pre-conditioned by an affective prelogic of race that functions on the psychic level of experience.” I frame Ekman’s emotional extraction as a form of “occupied emoting,” in reference to Fanon’s description of “occupied breathing.” Emoting that is occupied by colonial affects hinges on racialized misrecognition. Fanon’s contemporary relevance in surveillance studies draws attention to the affective dimensions of anti-Blackness embedded in surveillance technology.

Technological Imaginaries
Moderator: Margaret Warthon

Anneroos Planqué-van Hardeveld:

‘Regimes of (in)visibility: unpacking how Google advances its AI authority'

As ‘algorithmic security’ (Amoore & Raley, 2017) is gaining in perceived importance, traditional security actors are looking at the Big Tech to help them prototype their (machine learning) algorithms. With Google becoming ‘AI-first’, this company especially is regarded as an authority in AI. On the one hand, eager to reinforce - and capitalize on- this position, Google is taking a hyper visible role in the (ethical and explainable) AI debate, producing and sharing AI specific knowledge. On the other hand, Google seems to be trying to keep its AI projects with the US government under the table, silencing critical employees in the process. Instead of viewing the (in)visibility of the Big Techs as a methodological challenge to overcome, this article argues that the (in)visibility dynamics of the Big Tech are an essential part of how they construct and aim to advance their position as AI authorities, and that we need to study these regimes to shed light on the way in which voices are silenced or magnified in the process. To do so, I trace what was made (in)visible, by/to whom and how, to identify which (in)visibility regimes were (re-)constructed through and during the controversy around Google’s involvement in Project Maven.

Yung Au:

‘Selling an Imaginary: The Fantasy of Machine Guardians'

This paper explores the socio-technical imaginaries of AI-assisted surveillance that corporations sell to governments. In particular, it focuses on a handful of western companies that exports surveillance-as-a-service to territories in the majority world. What is included in the remit of AI-assisted surveillance is vast with countless grey areas yet recurring similarities exists in an otherwise patchwork landscape. In our rush to equip governments with the latest gait recognition systems and lie detection devices, we overlook the need to interrogate the impossible ideals that are shaping policing in various ways: what imaginaries are smoothing over potentially devastating kinks of these often under-developed systems? And what imaginaries are being exported along colonial and imperialist lines? Corporate entities have immense agenda-setting powers in shaping the supply but also the demand of government surveillance systems. They are able to give form to what is and is not possible through selling ideas, promises, and terminologies that obscure more than they reveal - much like how “cloud,” “platform” and “AI” are able to mean simultaneously so much yet so little. There is an urgent need to excavate how these fantasies of machine guardians and biometric gatekeepers, coloured in metallic silver and electric blue, are carefully packaged, embellished, sold and deployed.

Gabriele de Seta and Anya Shchetvina:

‘Imagining machine vision: How Chinese companies imagine and represent new sensing technologies'

Machine vision—the computational capability to interpret visual information—is more than a set of techniques and technologies: as an umbrella term for specific applications of artificial intelligence and machine learning, it also requires representational imaginaries and a constant work of articulation. Companies developing machine vision products employ visual media to showcase and illustrate their technological innovations, often relying on existing cultural codes, visual tropes and situated aesthetic contexts. In this paper, we conduct a social semiotic analysis of the official websites of selected Chinese tech companies that develop machine vision products (including, for example, facial recognition, object tracking, automated surveillance, etc.). By collecting, coding and comparing the use of various visual resources (such as icons, stock images, infographics, advertisement, video explainers) used on these webpages, we identify different sociotechnical imaginaries through which these companies represent, illustrate and imagine machine vision. Some of these imaginaries dovetail with how machine vision is represented in other global contexts: as a science-fictional “urban dashboard” (Mattern, 2015), or a reassuring provider of “infrastructural surveillance” (Gekker & Hind, 2020). Other imaginaries speak to China's social and political context, depicting machine vision as a key tool for pandemic governance or the ‘unmanned economy’.

*PANEL: AIPact Panel

Moderator: Ward van Zoonen

Tessa Oomen:

‘Trust Lies in the Eyes of the Beholder: Going Beyond Technical Solutions for Trustworthy Edge AI’

Edge AI is gaining popularity as a solution for real-time event analytics to autonomous self-driving applications. It is a domain that merges edge computing, data analytics and AI/ML that enables storage, computing, and AI functionality close to end users and their devices. It allows for improved data management flexibility, speed, governance, and resilience, compared to cloud-based solutions. While Edge AI seems to become embedded in many social and personal contexts, there are still uncertainties for end users related to surveillance, security, and privacy. Edge AI relies on end-user involvement for computational power but lacks clear descriptions of how end-users (or their devices) are involved in Edge AI systems, whether can opt in or out, how they are being monitored, and what control they might have (or not!) over their involvement in such systems. There is important ongoing work on transparency and trust around AI, but preliminary results of this digital ethnography-based study indicate that this is mainly approached through the principles of explainable AI. This neglects how end-user trust also depends on experiences and understandings of society. Thus, in order to improve trust holistically, AI developers should reflect on organizational and communication practices that affect end-user trust in AI.

Yasmine Ezzeddine, Saskia Bayerl, Helen Gibson and Tatiana Chelli:

‘Understanding citizens’ reactions to surveillance and artificial intelligence (AI) use by Law Enforcement Agencies (LEAs)’

The use of Artificial Intelligence (AI) by police forces is linked to expectations of improved crime prevention, detection and resolution (e.g., by optimizing evidence gathering and analysis process or by aiding the discovery of new crime trends and patterns). On the other hand, citizens raise legitimate concerns such as reinforcement of social inequalities, faulty decisions or inflexible, insensitive procedures that cannot be challenged because the underlying rules are too complex or opaque. In our study, we investigate the reasons citizens across six European countries (Germany, Greece, Netherlands, Portugal, Spain, UK) give for accepting or resisting AI use by police forces to fight cybercrime and terrorism. Using scenario-based semi-structured interviews, we identify highly differentiated acceptance and resistance rationales including conditions under which acceptances may morph into (passive or active) resistance. These are accompanied by clear expectations for specific safeguarding procedures as well as AI ownership (e.g., whether citizens should have access to AI systems for fighting cybercrime and/or terrorism). Our study illustrates the complex interaction between social/public good and individual motivations that shape reactions to AI use in the context of security including boundary conditions under which security may trump privacy considerations.

Marvin van Bekkum and Frederik Zuiderveen Borgesius:

‘AI and insurance: risks for privacy, non-discrimination and fairness - An interdisciplinary exploration’

Artificial Intelligence (AI) is increasingly used in the insurance sector. For instance, AI systems can help to predict where burglaries will occur, which drivers are more likely to have an accident, or which transactions are fraudulent. Insurers could use AI systems to set prices and to decide whether they offer somebody insurance. The increasing use of AI-driven segmentation in the insurance sector could also create problems. For instance, AI-driven segmentation may discriminate, accidentally, against people with a certain ethnicity. AI-driven segmentation could also make insurance unaffordable for some consumers, reinforcing social inequality. These problems have not yet been charted completely. This paper asks: When using AI in the insurance sector, what are the threats to fairness and to the rights to privacy and non-discrimination, and what can be done to mitigate the threats? We map the risks related to the use of AI in the insurance sector. Where we focus on law, we focus on Europe. Nevertheless, the paper could be relevant outside Europe too, as the problems in the paper stretch beyond country borders. We focus on what can be done by companies, supervisory authorities, policymakers, civil society, and academics to mitigate the problems in the insurance sector.

Youngrim Kim:

'There are too many liars": AI contacting tracing system and the culture of pandemic surveillance'

This paper examines South Korea's AI contact tracing system – "Epidemiological Investigation Support System (EISS)" – that has been nationally deployed as well as exported to other Southeast Asian countries during COVID-19. EISS is a centralized data platform used by human contact tracers to integrate and analyze patients' data extracted from different public and private institutions. When a positive case is identified, the system automatically visualizes the patient's recent trajectories – based on big data analysis of their mobile location data, credit card data, QR code check-ins, and CCTV footage – to expedite (or even replace) the phone interview process in contact tracing. Recently, the system has been upgraded to predict local "hot zones," and potential "risk groups" who are deemed more vulnerable to infection. Drawing from interviews with technologists, public health experts, human rights activists, and textual analysis of media and policy materials, this paper examines the sociocultural harms of this algorithmic system that has transformed established public health practices and governance. Illustrating how EISS is built upon deep distrust toward confirmed patients, I argue that this surveillance infrastructure became a massive vilification machine that displaces responsibility of infection control from the state to individuals, while disproportionately targeting marginalized populations.

*PANEL: BOLD CITIES (1): Co-creation of Urban Surveillance

Moderator: Vivien Butot

Rakshit Kweera:

'Smart City Surveillance Project in Hyderabad: A Participatory Model of Surveillance'

Hyderabad is reported as the second most surveilled city in the world. CCTV surveillance in Hyderabad is backed by laws and policies of the Telangana State Government. The A.P. Safety Act of 2013 provides Access Control mechanisms i.e., CCTV for establishments with a likelihood of public gathering of 100 people or more at a time. However, Hyderabad Police felt that this was not enough to deal with the menace of crime in the city and came up with two more programs, Nenu Saitham and Community CCTV Project. The former motivates shopkeepers and individual businesses to install CCTV in their premises and later residential communities. What we are witnessing is citizens participating and becoming a stakeholder in this smart city surveillance project. Recently these technological surveillance tools are also facing citizen's resistance. The existing CCTV infrastructure has been upgraded to facial recognition and is being used by police to unlawfully detect mask violators and randomly check citizens on the streets. In this paper, I will be looking at the rationale of smart city surveillance project by the police, interests of businesses, citizen's participation in this project, resistance which has surfaced lately as these mechanisms have normalised after the pandemic.

Donya Hatami:

‘Surveillance Discourses in the Canadian Smart City’

Increasing technological integration as part of urban design and governance is often framed around making our cities ‘smarter’, but it also inevitably makes our cities more surveilled, since the functioning of the smart city model requires continuous and extensive data collection. Despite increased surveillance being a necessary consequence of the smart city project, certain smart city narratives narrowly focus discussion on the utopic potential of technology to make our cities safer, more efficient, or more sustainable, with far less focus on potential risks. This research examines how urban surveillance is discursively constructed and rationalized, and considers how and why surveillance technologies have become so ubiquitous as a solution to problems of urban governance. I apply a governmentality approach to understand surveillance in the smart city as a political technology of urban governance and recognize how discourses of surveillance can be understood as systems of knowledge that constitute and shape the practices of government. This paper also draws upon the concept of urban, socio-technical imaginaries as a key part of discourse that informs dominant narratives. Focusing on the Canadian urban context, I demonstrate how discourses of the smart city rationalize surveillance practices and contribute to the endurance of the current ethos of urban surveillance.

Isaac Oluoch:

‘Intersecting Lines: Negotiating Values in the Surveillance of Slums’

Remote sensing technologies employing satellites, drones and GPS devices, along with machine learning and geo-data visualization platforms (e.g. OpenStreetMaps and Mapillary) are increasingly used to represent spatial and social information captured from slums on digital maps. The need for representing this information stems from epistemic gaps concerning knowledge of slums (i.e. their morphology, levels of health, income and poverty), to meet Sustainable Development Goals (SDGs) 3 (promoting public health), 6 (access to water), 11 (safe, inclusive and resilient cities) and 13 (climate adaptiveness). While remote sensing technologies have the potential to close these epistemic gaps, they also raise some concerns regarding the increasing surveillance of slums and slum dweller communities. The actors involved in acquiring information on slums have respective values and goals which intersect with each other (e.g. increasing medical knowledge, protecting the privacy of slum dwellers, empowering the political capacities of slum dwellers, or designing the geo-information system to be inclusive and participatory). This paper will investigate how the intersecting values and goals that exist between the actors involved in the deployment of remote sensing technologies, are negotiated in the surveillance of slums to reduce epistemic gaps and meet SDGs 3, 6, 11 and 13.

Marc Schuilenburg and Yarin Eski:

‘Luxury Surveillance: On Tesla and Silent Lethality'

This paper analyses the increasingly influential role of tech companies in designing and deploying smart luxury surveillance in private vehicles. In using the case of Tesla, a company that makes optimistic promises and hopeful visions for more sustainable electric cars by decreasing the ecological footprint, the problematical aspects of artificial intelligence (AI), big data and algorithms as total-surveillance by private companies will be discussed. Moreover, in particular the issue of discourses on sustainable and smart vehicles that dim the light on smart surveillance, will be shed light on. As will be made clear, Tesla's green and lean – aspirational – ambitions through different technological and surveillance advancement, make old forms of control revive and introduce a new set of power/knowledge relations. Beyond the question of privacy and personal data harvesting, this paper discusses the wider social and political consequences of smart car luxury surveillance by private companies.

*PANEL: BOLD CITIES (2): Contending Imaginaries of Urban Surveillance

Moderator: Liesbet van Zoonen

Vivien Butot:

'Scored data walks: performatively studying subjective experiences of smart city surveillance'

Smart cities are seen as places that are defined by surveillance because of their reliance on vast amounts of digital data to improve urban management challenges. Although the infrastructures and technologies that enable smart city surveillance pervade multitudinous urban spaces and everyday practices, they are often 'hiding in plain sight', going unnoticed in the bustle of everyday life. Hence, fostering research settings where participants can productively reflect on their everyday surveillance constitutes a major challenge for empirical research about subjective experiences of smart city surveillance. Drawing on scholarly and artistic methodologies that employ performativity, this study attempts to meet this challenge by developing and empirically testing a hybrid methodology of scored data walks.

Situating the research in Rotterdam, the Netherlands, participants are instructed to perform short walks through the city to identify data points for public safety purposes and reflect on their experiences. Observations and experiences of smart city surveillance are documented with photos, text descriptions and audio notes, which are shared in real-time with researchers, and provide the basis for collective reflections. These performances and reflections generate rich visual and textual data, reflecting active constructions of smart city surveillance as an object of subjective inquiry, surfacing experiences of visibility, evaluations of public safety implications and considerations of agency. The study considers these empirical results in conjunction with reflections on the methodology, contributing to further methodological explorations of surveillance subjectivity research.

Debra Mackinnon and Sava Saheli Singh:

'Vulnerable Bodies: Relations of visibility in the speculative smart city'

Through wearables, IoT sensors, apps, platforms and cameras, we “shed” various forms of data as we navigate our increasingly networked and smart environments. Recent discussions of urban data have focused on post collection practices of translation and circulation – following data threads, journeys and exhaust as they enact urban life. We seek to further complicate these thick data accounts focusing on movement, bodies and embodiment. As our bodies become information, the accuracy and affordances of these data portraits remain critical sites of inquiry. How do surveillance technologies map, render and make visible human and non-human interactions? Adding to the rich discussions of future-ing, anticipatory imaginaries and implications on the urbanite body, we offer a critical interrogation of the oligoptic gaze and the relations and politics of visibility. We do this through the narrative of Frames [https://www.sscqueens.org/projects/screening-surveillance/frames] – a speculative near future account of mapping a body through the various lenses of a smart city. Focused on what is included (and excluded) from the “frame”, we navigate domains of aesthetics and politics in order to foreground the embodied experiences, decisions and interactions which are mapped by these surveillant spatial locative technologies. We contend these renderings or simulacrum of a ‘singular’ knowledge politic serve to normalize ways of seeing, knowing and control, potentially producing inefficient, inaccurate and unjust portraits.

Stephanie Garaglia and Lander Govaerts:

‘Unfolding urban reality: Towards a reconceptualization of violence through smart surveillance’

Urban spaces have become a growing network of (in)visible subsystems that continuously (re)create, maintain, and contest power and subjectification. The drive to make these spaces smarter, created a surveillance network that is increasingly woven into the city’s fabric. Smart surveillance technology progressively commodifies the urban dweller. Therefore, traditional forms of violence, inherent to capital accumulation, are extended by the rise of surveillance capitalism that pushes the boundaries of accumulation into areas of control. This capitalization of our being is increasingly difficult to resist. Data is irrespectively extracted and used by new forms of (in)visible smart city surveillance to alter current and future urban processes on different levels. This demands a reconceptualization of violence in the city, as questions arise about what is left of us: the people who work, live and move through the city. By using ‘the fold’ of Deleuze as a toolbox to grasp the current state of subjectification of city dwellers, the implementation of smart surveillance technology will be brought to account. This paper seeks to provide an insight into how people in Western democratic cities can make sense of themselves as they undergo and/or act upon this new and rapidly changing urban reality.

Irena Barkane, Anda Adamsone-Fiskovica and Emils Kilis

‘Interrogating visual digital surveillance in road traffic control'

The paper critically analyses the visual surveillance in road traffic control and its societal and legal ramifications, with a specific focus on speed cameras, smart 360-degree cameras in police cars, drones, and smartphone apps in Latvia.

First, the paper explores the changing relationship between individuals, traffic and the police in public spaces and explores how these visible and concealed forms of visual surveillance are framed by different stakeholders in terms of prevention vs. punishment and how police powers vis-à-vis citizens are being exercised through the use of these tools.

Second, it examines the perceived adequacy of the tools in the light of their postulated goals as well as the concerns raised by their practical applications and possible future uses. The paper argues that while the use of traffic surveillance tools is becoming more prominent, allowing to save police resources, they may not necessarily be the best solution if road safety is the intended long-term result.
Finally, the paper explores to what extent is the use of these tools regulated or lacks regulation and emphasises the need to adopt a regulatory framework that sets out procedures for assessment, use and monitoring of both new and existing surveillance technologies.

PANEL: Affective Surveillance through Emotional AI in Smart Cities

Panelists:

Diana Miranda
Lachlan Urquhart
Andrew McStay
Vian Bakir
Peter Mantello (Chair)

Emotional AI (EAI) technologies are emerging in our daily lives in both public and domestic spaces. EAI enables new forms of emotion based surveillance through advances in machine learning and biometrics. Techniques such as off body facial feature sensing and sentiment analysis seek to infer intent of subjects; and on body physiological sensors reading heart rate and galvanic skin responses seek to more intimately interpret mental state. Such technologies are emerging as new analytic layers in a range of domestic applications, such as wearables and smart toys and scale to wider scale uses in edtech, public space advertising and policing. We are concerned about the role of emotion sensing technologies in mediating our everyday lives, particularly as the scientific models of emotion underpinning these systems are contested. The regulatory challenges, the democratic implications, and need to understand how EAI changes the nature of state and private surveillance are all key areas of concern. The panellists will discuss the implications of using EAI in different settings, particularly for commercial, civic, security and policing. They will present both the ‘big picture’ of how these technologies have emerged, provide examples of their use, and highlight key concerns to date and present complementary empirical and conceptual research activities. This includes on: UK police perspectives on use of EAI; how EAI is going to be integrated into the automotive sector; and its role in microtargeting and social media disinformation. The group of panellists is highly interdisciplinary, bringing perspectives from criminology, sociology, law, computer science, media and journalism. The panel will raise awareness of how EAI is being used to detect behaviour and the ethical, legal, and socio-technical questions that need to be addressed. The panellists will also draw on their engagement with diverse EAI and smart city stakeholders in both UK and Japan including industry, policymakers, policing practitioners, civil society and citizens. Ultimately, this discussion contributes to ongoing debates in surveillance studies, namely in relation to urban surveillance and biometrics, and how to ‘live well’ with emerging affective surveillance technologies.

Nature & Sustainability

Moderator: Jeffrey Monaghan

Francisco Klauser:

‘Big Brother meets Animal Farm: A Research Agenda on the Surveillance Implications of Smart Farming’

Farming today relies on ever-increasing forms of data gathering, transfer, and analysis. Think of autonomous tractors and weeding robots, chip-implanted animals and underground infrastructures with inbuilt sensors, and drones or satellites offering image analysis from the air. Despite this evolution, however, surveillance studies have almost completely overlooked the resulting problematics of power and control. This presentation offers a review of the main surveillance issues surrounding the problematic of smart farming, with a view to outlining a broader research agenda into the making, functioning, and acting of Big Data in the agricultural sector. For surveillance studies, the objective is also to move beyond the predominant focus on urban space that characterises critical contemporary engagements with Big Data. Smart technologies shape the rural just as much as the urban, and smart farms are just as fashionable as smart cities.

David Murakami Wood:

‘Anthropocene Surveillance’

In the Anthropocene–the era of humanity– the focus of society and politics is shifting towards the planetary scale and questions of the survival of humanity and life on earth. This paper explores the concept of "anthropocene surveillance," combining thinking on globalization of surveillance, with planetary urbanism, planetary computing and the growing planetary environmental crisis. Surveillance is crucial to this new condition, with AI-driven, smart infrastructure envisaged as interpenetrating existing social and ecological systems. We are increasingly living with(in) a "vast machine" (Edwards 2010) of modelling and sensing technologies for environmental management, and surveillance technologies for social ordering. Surveillance "for our own good" has become familiar during the COVID-19 pandemic but the climate crisis is of another order of magnitude, and surveillance changes with scale and space, and for diverse communities, especially if the stakes are higher and the consequences invisible, beyond the horizon, or unevenly distributed - the results, for example, of both historical and ongoing racism, capitialism, colonialism and dispossession. This paper will aim to discuss the big questions relating to anthropocene surveillance, including the political economic and political ecological implications; the likely impacts on human rights and justice; and what descriptive and empirical and theoretical questions we need to ask to identify emergent trajectories and conditions for change.

Henry Osman:

'From Leaf to Bomb: Plant Nanobionics and the Operationalization of Ecology'

In 2016, DARPA initiated its Advanced Plant Technology (APT) program to develop energy-independent plant sensors. New techniques in plant nanobionics transform vegetation from a subject of war into a field of operations in and of itself, reimagining the agentic capacity of the vegetable world. Wild spinach plants might become able to detect landmines, enemy movements, or even electromagnetic signals, a particular goal of DARPA's project. These efforts map onto a long history of vegetable intelligence, from CIA experiments in plant biofeedback to Operation Igloo in the Vietnam War. Upon apprehending and processing these environmental stimuli, nanobionic plant leaves light up with fluorescent dots visible to infrared cameras. I term this a 'vital informatics,' a living information science that integrates organic systems into processes of data collection, storage, and processing. Nanobionic spinach is designed to be integrated into drone surveillance networks, uniting plant and animal intelligences. Ecological relations between different species are themselves operationalized as information displaces energy in the trophic web. Attuned to the current limitations of APT and the bellic ecology it portends, I contend that APT ecologizes warfare by understanding the biosphere not as background and battleground but as a force and a front of its own.

Catherine Brooks and Sarah Young:

'The Importance of Absence: Information, Surveillance, and UN's 2030 Agenda for Sustainable Development'

A key concept of surveillance is the idea that information is gathered about individuals to be turned into applicable intelligence. As Lyon (2007) defines, surveillance can be understood "as any systematic, routine, and focused attention to personal details for a given purpose" (p. 13). Information then, as an object of inquiry, is an important concept to study. For a robust study of surveillance, it is also important to understand not just the sites, technologies, or processes which facilitate data and information gathering (Ball, Haggerty, & Lyon, 2012), but it is also important to see the ideological positions that allow surveillance to proliferate and which allow information to be gathered (Young, 2017). This angle helps identify the tracks of surveillance. While this can include the materialization of surveillance through public policies (Raab, 2012) and global discourse which spell out the constraints and limits of surveillance capabilities (Aas, 2009), it can also include the absence of attention to principles of surveillance in these spaces as well. Paying attention to absence is a way to see the unseen. With this premise in mind, this study focuses on the UN's 2030 Agenda for Sustainable Development. By examining the agenda qualitatively, we illuminate how information is situated discursively in the new agenda. We argue for a more focused consideration of the sustainability of information collection, with special emphasis on related privacy and surveillance issues in a digital world. This has larger implications for surveillance scholars because it provides foresight into the work needed to be done to affect attitudes and future policies.

Crisis, Vision & Privacy
Moderator: David Murakami Wood

Torin Monahan:

‘Crisis Vision: Critical Surveillance Art and the Racial Order'

In this presentation, I develop the concept of “crisis vision” to describe a pervasive, destructive way of seeing that amplifies differences among individuals and inspires the scapegoating of those marked as Other. Crisis vision festers within the inherent contradictions of liberal humanism. Rights have never been apportioned equally and in fact have been secured for some through their denial to others. To the extent that racial subjugation serves as a constitutive feature of societies, not merely as a passing exception, then crisis-vision regimes can be seen as reproducing and regulating white-supremacist racial orders. Surveillance is both a weapon of and an outlet for crisis vision; it provides a way to activate racial divisions while grounding them in a seemingly rational and objective institutional foundation. I draw upon critical surveillance artworks to present these dynamics for contemplation and revision. The artworks that make the greatest incision into the social, I argue, are those that confront white supremacy and destabilize racial hierarchies through performances of opacity.

Marie Eneman, Jan Ljungberg and Bertil Rolandsson:

'Secret Data Interception' and its implications for privacy'

Emerging technologies are laying the ground for surveillance capabilities of a magnitude we have not seen before. This study focuses on the implementation of the new Swedish law 'the Secret Data Interception' which means that the police and other law enforcement authorities now have been given an extended mandate to use powerful surveillance capabilities as part of their government work. The law gives the police the right to secretly enter e.g. computers, mobile telephones or user accounts for storage or communication services for reading or recording data contained in the physical equipment or service and allowing the activation of a camera or microphone in a technical device to capture sounds or images from a suspect but with risks that also non-suspects can be included. The introduction of the law is motivated by more effective law enforcement and increased security, while there is a strong concern for citizens' privacy as this gives the state a legal right to far-reaching surveillance and control. According to current law, the police and other law enforcement authorities are always obliged to weigh their need and interest against citizens' right to strong privacy protection. The following two questions have guided this study: (i) What implications does the new law have for citizens’ privacy? (ii) How do law enforcement authorities ensure strong privacy protection for citizens when using secret data interception?

Jennifer Gradecki:

'Informational Mosaics and Thinking Machines: The Technical Metaphors of Dataveillance Practices'

Two of the most prevalent metaphors used by intelligence analysts—the mosaic metaphor and the computational metaphor of mind—frame dataveillance in ways that lead to the mass collection of data and the automation of the analytical process. When intelligence analysis is conceived of as mosaic building, it becomes necessary collect every potential piece of the mosaic, leading to a 'collect it all' mentality and exacerbating the problem of information overload. The computationalist metaphor of mind bilaterally conceives of the analysts' enigmatic mind as computer-like and automating software as resembling the analysts' mind. Together, these technical metaphors provide the conceptual foundation for a belief in the value of mass dataveillance and the use of artificial intelligence to automate intelligence analysis. Data analytics companies and government contractors who can implement automated dataveillance have monetary and even existential reasons to perpetuate the mosaic and computational metaphors: these metaphors allow them to market their technologies and services as the solution to information overload. Left unconsidered, the assumptions underpinning these technical metaphors could become the basis for the development and implementation of new dataveillance techniques and technologies that perpetuate problems like information overload and statistical errors that lead to false positives and negatives.

PANEL: Reconsidering the Trace: Alternative Surveillant Epistemologies

Panelists:

Katherine Chandler
J.D. Schnepf
Hillary Mushkin
Nina Franz
Andrea Miller (Chair)

Targets, tracks, and traces permeate contemporary technical, state, and everyday discourse: they are aligned not only with contemporary war and policing but also with forms of knowledge-making (Weber, 2005), image production, and the very terms of sensibility itself (Kaplan, 2017). This panel reconsiders intersections between surveillance, seeing, and knowing to examine enactments of control through ostensibly omnipotent mechanical means. Drawing out the ways such practices produce uncertainty, unknowability, and unpredictability, we propose possible counterpoints to and lines of flight from dominant surveillant modalities of governance and knowing. We apply feminist and postcolonial theoretical approaches to destabilize sociotechnical systems and objects that range from the drone to cybersecurity to protocological techniques of computation. In doing so, we take seriously the definition of the trace as "what is left behind" or that which cannot be removed completely. The panelists read for these traces in the material affordances of the classified document, the contingency of the non-automatable human, the excessiveness of the target, and the insurgency of the microgesture. In their contribution "Drone Archive," Kate Chandler and Hillary Mushkin take up the relationship between data, machine, and death through the materiality of US drone warfare and its interconnection with daily life. While Chandler and Mushkin engage processes of tracing and sketching to think about the targeted image, panelist J.D. Schnepf considers how the figure of the feminine subject in comedies, police procedurals, and cartoons inadvertently upturns conventional epistemologies promised by the police-piloted small unmanned aerial system. Shifting our attention to cybersecurity, Andrea Miller charts how embodied “microgestures of dissent” (Adeyemi, 2019) function as political traces of subjectless refusal to the implementation of cybersecurity-driven surveillance and redevelopment practices in the city. Finally, drawing on contemporary philosophy and the recent history and theory of protocols, Nina Franz seeks to open discussion on changing concepts of surveillance, where the non-predictable is no longer understood as antagonist or error but as an extractable resource. Through an attention to alternative and embodied epistemological practices, panelists reconsider what forms of knowledge might ensue when not predicated on a surveillant impulse toward totalizing authority.