States of Surveillance Symposium, October 2,
Malott Room, Level 6 Kansas Union
University of Kansas

9.00am

James Walsh, Assistant Professor, Social Science and Humanities, University of Ontario Institute of Technology
<James.Walsh@uoit.ca>

"Mass-mediated Surveillance: Borders, Mobility, and Reality Television"

In the post-9/11 period the surveillance of borders and mobility is not only being escalated in the name of national security, but also represents an emerging dimension of popular culture and object of intrigue, amusement, and desire. This article assesses these trends by analyzing the social construction of border policing and surveillance in reality-based television programs. Relying on content analytic methods to document and decode mass-mediated images of borders, crime, and insecurity it assesses the cultural meanings and ideological character of border-based reality television, focusing on three programs: *Border Security: Australia's Front Line; UK Border Force;* and, the American program, *Border Wars*. Despite claims of featuring unfiltered, unscripted, and authentic depictions of 'the real', all three programs provide distorted images of border enforcement that reinforce stereotypes regarding the risks of cross-border movement and exonerate intensive regimes of surveillance and securitization.

Nicholas Lustig, Assistant Professor, Geography, SUNY Buffalo
<nflustig@buffalo.edu>

"The Variegated Mobilities of Surveillance Policies: The Spread of Real-Time Crime Centers"

This paper adapts the work of Jamie Peck, Neil Brenner, and Nik Theodore on variegated neoliberalism and policy mobilities for the study of surveillance and systems of power. It begins by identifying some key principles in the work of Peck, Brenner, and Theodore and making an argument that while their work is focused multi-scale forms of capitalism and neoliberalism, many of their principles of analysis can and should be extended to studies of power more generally. A series of principles for the study of 'variegated systems of power' is presented. Next, this paper examines the presence and absence of these principles in the work of Foucault on disciplines, Deleuze on control societies, and Bogard on hypersurveillant simulations. Finally, this paper ends with a discussion of how these principles can be used to analyze the spread of Real-Time Crime Centers from New York City to cities around the country, including Chicago, Houston, and Los Angeles. Emphasis is placed on how a model of variegated power can help focus attention on how Real-Time Crime Centers, while becoming core operating systems of police departments around the country, display significant levels of diversity within local contexts and mutate as they move across the country.

10.00am

Cristina Blasi Casagran, Lecturer, School of Law, Autonomous University of Barcelona
<Cristina.Blasi@uab.cat>

“The Need to Define ‘National Security’ In the EU and the US”

In the EU and the US there are laws protecting the rights to privacy and information even when data are collected and processed for the prevention and combat of crimes. Yet, the majority of these laws exclude data collected and used for ‘national security’ purposes. What does this term mean? Does it enclose all activities conducted by intelligence services? This paper seeks to analyse the problems emerging from the lack of a clear definition of the concept ‘national security’. It examines the main challenges in the EU and the US laws and case-law regarding the blurry scope of this term. Particularly, it focuses on the relationship between the concept ‘national security’ and intelligence services’ activities. It will also analyse whether individual rights such as the right to privacy and the right to information might be ultimately restricted by invoking ‘national security interests’.

10:30-10:45am Break

10:45

Don Haider-Markel, Professor and **Steven Sylvester**, PhD Student, Political Science, University of Kansas
<dhmarkel@ku.edu>

“The Role of Anxiety and the Evolving Balance between American Support for Civil Liberties vs. Extensive Counterterrorism Policies”

Although Americans support protection of civil liberties in the abstract, after the attacks of 9/11 Americans were more willing to support counterterrorism policies that impinge on civil liberties. Some research indicated that individuals that were worried about their own safety were less likely to support strong counterterrorism measures, but those worried more generally about the country being attacked were more likely to support strong counterterrorism policies. Our project explores American support for counterterrorism practices that engage surveillance technologies and examines whether the relationship between worry about terrorism and support for counterterrorism practices persists, especially following the 2013 revelations about National Security Agency programs. We employ data from several nationally representative surveys to examine this question. Our analyses suggest that Americans have become more supportive of protecting civil liberties in the fight against terrorism, but individual beliefs about the threat of terrorism still strongly shape support for counterterrorism measures. We discuss the implications of our findings for the future of civil liberties protections.

11:15am

Rachel Dubrofsky, Associate Professor, Communications, University of South Florida <rdubrofsky@usf.edu>

"Under Surveillance: Mediating Race and Gender"

This presentation discusses a book project underway, which approaches the analysis of surveillance and media via a focus on both contexts of surveillance and media spaces that are not under surveillance but where an ethic of surveillance is present. Specifically, in these contexts, the book looks at notions of authenticity, performance, and self-reflexivity, examining the critical implications for racialized and gendered identities and bodies. The work moves beyond surveillance technologies and contexts of surveillance to theorize a culture of surveillance, asking: What kinds of spaces are created under surveillance? What new insights might be gained by situating visual surveillance technologies alongside visual media? In what ways does the increase in spaces of surveillance—both those inhabited by people in their daily lives (social media, for example) and those featured in popular forms of media (reality TV, for instance)—privilege behaviors that extend beyond surveilled spaces? What is enabled within these spaces? What is privileged? How might these privileges and possibilities be attached to racialized and gendered bodies and identities?

Simone Browne, Assistant Professor, African and African Diaspora Studies Department <sbrowne@austin.utexas.edu>

"Black. Life. Forms"

This talk will look at escape, the technologies of tracking blackness in the archive of slavery (from the slave ship *Brookes*, ledgers and runaway notices to biometrics), to discuss how anti-colonial practices can continue to inform a critique, and sometimes rebellion, when it comes to contemporary surveillance.

12:15pm Lunch

1.30pm

Aaron L. Fister, PhD Student, Political Science at the University of Oklahoma <aaron.fister@ou.edu>

"Expanding the View: Trust in Security Administrative Agencies"

The intersection of government trust, threat perception and perceived implications of advanced technologies for privacy provides a unique basis for testing propositions about the determinants of public trust for governmental institutions. Utilizing national survey data, this study explores factors that influence trust for specific agencies' domestic use of unmanned aerial vehicles (UAVs -- also known as drones). Substantial differences exist in mean levels of trust for specific agencies. Generic measures of trust for the federal government and perceptions of the threats posed by terrorists, have similar levels of influence when comparing trust for agencies' use of

UAVs. The implications are that, when explaining variations in trust, theories and models that include both general and agency-specific explanations will be needed.

Andrew Fisher, PhD Student, Sociology, University of Missouri
<arfxvc@mail.missouri.edu>

“Differing Values of Anonymity among U.S. Patriots and Anonymous”

This paper outlines the differing ways political groups respond to anonymous researchers prying into their online activities. As a part of my dissertation, I have been profiling U.S. Patriots and Anonymous. Under anonymous handles in Internet Relay Chat (IRC), social media websites and Internet radio shows I have engaged them steadily for over three years, interacting with these groups in varying degrees. Some Patriots are willing and excited about my presence, offering personal details about themselves and their groups without much suspicion to my motives, whereas others quickly ban my communications with the slightest sense that I do not belong. Similarly, Anonymous venues react differently to my presence; anonymity is a more valued portrayal of identities. Details about oneself are often considered suspicious and have at times been cause for dismissal from group interaction. The differing ways groups allow strangers into their circles is telling, not only their politics but, of how they understand the undertaking of their political activity. U.S. Patriots are more willing to divulge personal information, but also respect my desire to remain anonymous. Anonymous, on the other hand, are much more apprehensive to indulge personal identities in Anonymous settings and usually require other locations of communication.

2.30pm

Noah McClain, Assistant Professor of Sociology, Illinois Institute of Technology
<nmcclain@iit.edu>

“Urgency, Fantasy and Failure: A Technological Security Fix in the New York Subway and the Gulf Across the Implementation Line”

This paper examines problems entailed in the actual adaptation of surveillance technology within the organizational and physical context of the New York Subway, and its operator, the MTA. Looking behind a veil of secrecy, I track the MTA's flirtation with, commitment to, and eventual dissolution of a technological security program. Following the creation of a security office in late 2001, security managers were given the imperative to 'do something' about the system's vulnerability, and improvised without any particular guidance from established security actors. Restrictions on funding directed them to capital projects and, in turn, a technological security solution. As I show, a number of imaginative proposals failed principally because they could not be normalized within the organization's usual way of accomplishing capital projects, leading eventually to one which could: a commitment of a half-billion dollars to a military contractor to develop a nonexistent 'smart surveillance' software for analyzing problematic human behavior in the subway environment. This program, in turn, failed against the practical obstacles entailed in machine learning algorithmic analysis of a socially and behaviorally heterogeneous setting, applied in a sprawling environment with few vistas. The case illustrates how organizations facing uncertainty and perceived crises of vulnerability may furtively default to heavy-handed technological solutions, even against deep doubt in their efficacy. The case also problematizes

the vast gulf between technologically-feasible surveillance systems and their implementation in actually-existing settings.

3.00-3:15pm Break

3.15pm

Torin Monahan, Professor, Communications, University of North Carolina
<torin.monahan@unc.edu>

"Built to Lie: Technologies of Deception, Surveillance, and Control"

This paper argues that deceptive communication systems are hidden articulations of normal technological orders. They are polyvalent and polyvocal; they are oriented toward surveillance and control, especially in their hidden functions; and they are commonplace and typically legal. Examples include things like untrustworthy hotel and workplace thermostats, applications to spy on workers and family members, and commercial and law-enforcement systems that surreptitiously collect mobile phone data. If deception in itself is not the primary problem with such systems, or with communication more broadly, as I suggest, then transparency alone cannot be the solution. As troubling as institutional opacity might be, more fundamental problems revealed by deceptive systems are imbalances in power and widespread acquiescence to corporate and state efforts to control individuals, groups, and their data. Accepting that technological veracity is always a fallacy and that untrustworthiness is the norm for all technological systems could redirect attention to power inequalities and the pressing question of how to live together ethically.

Keith Spiller, Post-Doctoral Research Associate, The Open University Business School, United Kingdom
<keith.spiller@open.ac.uk>

"Wearable Devices: Why People Collect Personal Data and How They Value the Privacy of Their Data"

Wearable technologies and quantifying personal activities are enjoying unprecedented levels of engagement, for example, Nike's fitness app, we are told is 'your personal trainer' which provides the motivational drive to keep you training. The logging of personal data through such devices and through what has been called the Quantified-Self (QS) - the logging of personal data by wearable technology users – has been shown to offer many benefits. Less well known however are reactions to the use of QS data by the suppliers of wearable devices. In this paper I concentrate on the values attributed to QS data, especially the value of the data in terms of encouragement and also in terms of the protection (or not). The paper asks two critical questions: 1) why users collect the data they do; and 2) what importance is placed on the data by users. Using evidence taken from interviews with QS users the paper reviews privacy and transparency in relation to personal data and offers an empirical perspective on how QS users consider the data they collect, and often display publically, as well as their attitudes toward the handling of their data by the manufactures of wearable technologies.

Elaine Sedenberg, John Chuang, and Deirdre Mulligan, PhD Students, UC Berkeley School of Information
<elaine@ischool.berkeley.edu>

“Promoting Public Good Uses of Privately Held Sensor and Device Data through Ethical Data Management and Information Sharing Practices”

The proliferation of sensors and Internet-enabled devices comes with unprecedented power to analyze aspects of behavior, health, and community patterns over extended periods of time. As users increasingly opt-in to using smart devices and biosensing wearables, private companies will cultivate a continuous and systematic repository of information rich and sensitive data. The ability to combine data streams across devices for unforeseen uses holds the potential to create new—and often invisible—surveillance regimes.

Data surveillance systems, like those within public health, harvest the power of large-scale reporting in a way that promotes public good uses, individual privacy and autonomy, information sharing between diverse organizations, community input, and increases the research utility. As these sensor systems mature, we propose the early integration of practices that promote responsible data management and sharing. We discuss design and management practices found within public health, and apply ethical and privacy principles to the unique challenges and opportunities of privately held user data. We propose elements of transparency, information sharing enabled through dynamic informed consent and limited access protocols, and incentives to promote adoption across organizations. Enabling the public good potential of these distributed data systems will promote a wider range of R&D and stakeholder activities.

6:00p-6:45pm Reception in English Room, Level 6, KU Student Union

6:45pm-8:oopm Dinner in Centennial Room, Level 6, KU Student Union