UNIVERSITATEA
ALEXANDRU IOAN CUZA

Living in Surveillance Societies

Ghosts of Surveillance
LiSS Conference 2
Iasi, Romania,
3-5 May 2011

Living in Surveillance Societies Annual Conference 2, Alexandru Ioan Cuza, University of Iasi, Romania, 3-5 May 2011.

ABSTRACTS

cost

UNIVERSITY OF STIRLING

Keynote Papers

Jens Linge
Detection of public health threats via media monitoring
Epidemic Intelligence comprises early identification, verification, assessment and investigation of potential health threats combining indicator-based and event-based approaches. Whereas public health authorities have routinely used indicator-based surveillance (IBS) systems for decades to gather structured data on infectious diseases, event-based surveillance (EBS) systems have only recently become part of standard epidemic intelligence activities. In my presentation, I will give an overview of automatic and moderated EBS systems and show the Medical Information System (MedISys) which is part of the Europe Media Monitor (EMM) family of applications. MedISys is a fully automatic EBS system which monitors reporting on human, animal and plant diseases, chemical, biological, radiological and nuclear (CBRN) threats, and food & feed contaminations. I will then discuss the challenges ahead: information extraction from publicly available social media, monitoring of audio transcripts from radio & tv, machine translation software, integration of indicator-based data, and collaborative tools for risk assessment.

Ivan Szekely
The role of remembering and forgetting in a world of increasing surveillance in the context of post-communist societies
The identity of individuals, groups of people and societies (heavily) depend on the sensitive equilibrium of remembering and forgetting. The post-communist (in general, change-of-the-system) societies are especially vulnerable in this context: when speaking about the need of remembering the past, we tend to disregard both the negative effects of arbitrary remembering, and the surviving culture of surveillance and collecting information about the civil sphere. This keynote will address the problems of distinction among personal information created in different social (public and private) roles, the dangers of the “eternal memory” envisioned by new and emerging technologies and those applying them, and the need for re-introducing selection and evaluation of personal information intended for preserving in the long term.

Conference Themed Workshop Papers

Doina Balahur and Adrian Iftene

I see you, you can’t see me: On people’s perception about surveillance in post totalitarian Romania

In this paper we present the outcomes of an interdisciplinary, exploratory research about people’s perception on surveillance in post totalitarian Romania. Our evaluation is based on opinion mining and sentiment analysis. Sentiment analysis, i.e. the analysis and classification of the opinion brought by a text towards its subject matter, is both a form of Internet surveillance and a form of information extraction from text of growing research and commercial interest. A sentiment analysis system should be able to extract sentiments and opinions from daily terabytes of unstructured data (blogs, newspapers, comments, forums, social networks) and to pinpoint on Who, Where, What and When someone says about a company/product/service, while excluding irrelevant, opinion-free sentences that keyword-based systems wouldn't. For purposes like monitoring the Internet before, during and after a campaign/message release, obtaining consumer feedback on different topics/products are the main applications that this system experiments with. The study that we present in this paper is to identify Romanian users' opinions and feelings in communication using

simultaneously classical methods that either phone or mail, as well as new methods like blog, chat or SMS.

Jelena Budak, Ivan-Damir Anić and Edo Rajh
Public attitudes towards surveillance and privacy in Croatia
This paper investigates public attitudes towards surveillance and privacy in Croatia. Croatia as one of the republics of ex-Yugoslavia had a quite different socialist political system compared to authoritarian communist regimes in other Eastern Europe countries. However, to insure political discipline and social stability some mechanisms of government control had been put in place. In the new era of independent Croatia, the transition and EU-accession process seem to shift the public interest to more transparency, while privacy protection issues might be neglected and surveillance memories vanished. There is no empirical study of citizens' attitudes towards surveillance and privacy issues in contemporary Croatia, and this research provides a unique evidence. The survey data collected on the sample of 500 respondents enabled us to examine the citizens opinions on surveillance and privacy intrusion, to identify the factors of surveillance/privacy concerns, determine the segments of population with similar attitudes, and to analyze the segment differences. Each item in the questionnaire was measured by Likert-scaled items, ranging from 1-strongly disagree to 5-strongly agree. The analysis is based on descriptive statistics, exploratory factor analysis, Cronbach alphas calculation, chi-square difference test, analysis of variance (ANOVA) and cluster analysis. Findings are expected to foster the discussion on government regulation and commercial activities related to the surveillance and privacy protection in Croatia.

Paul Dobrescu
Ethical issues and surveillance societies
This paper approaches some ethical issues raised by the culture of surveillance. The undertaken inquiry relies on the classical work of Weber and Foucault and also on the more recent analysis developed by Christie, and Bauman. Based on different research studies the paper emphasizes that surveillance was (and is) a ubiquitous culture born as 'fruit' of modernity itself, promoted with different 'means' both by western and eastern regimes, but with the same aim of 'identifying and codifying the enemies'. Are there differences between manipulation by ideologies as "sexual liberation", "Beatles experiment" or "preventive contra-revolution" and the 'eastern gulag'? Are there legal and ethical 'differences' among the experiments of lobotomy and the enforced disappearances of the dissents? The paper underlines that for the democratic societies, the culture and ethics of civil and political rights have been important barriers that, at least apparently, prevented abuses and gross violations of human rights. For totalitarian societies the remedy seemed to be 'the retreat in Epicure's garden' accompanied by a strong self-control-surveillance. The paper asks what happens today when the 'total surveillance' practices and strategies supported by technology is re-legitimized, especially after 11/2001, by the need to provide citizen's and community safety ?

Katalin Parti
The lives of others. Conceptions on post communist countries' attitudes towards surveillance
The presentation studies the revival of „surveillance societies" in the 21st century. The now adult population of the post-communist societies had perceived everyday life surveillance on (or under) its own skin. According to one hypothesis, this experience has lead to „habituation", i.e. such a customization that makes adult population living in nowadays' post-communist societies not consider new forms and techniques of surveillance (collection of personal data, interconnectivity of databases, „open lives") initiated by today's democratic governments as a deterioration of freedom, or to say the least the population is not so against it as the older democracies. As per the other hypothesis however, there has not been a „habituation", but on the contrary, a „dishabituation"

process passing off in post-communist societies according to which grievances and unfavourable undergoes of the past resulted in a higher level of sensitiveness and a lower level of tolerance towards newly introduced means of surveillance. How do citizens in post-communist countries really feel about the „second hype of surveillance" after the transition? The presentation seeks to find answers to this question. I will call literature, film and media examples for help in order to demonstrate possible scripts of post-communist societies' attitudes towards nowadays' surveillance actions. The task on the other hand is to represent countries' different reactions (post-communists and others) called upon by the Directive 2006/24/EC of the European Union on data retention. The different solutions and views are to be (com)pared by the findings of Eurobarometer surveys on the overall satisfactory level, and the different stances for and opinion of the data protection issues of the population.

Minas Samatas, Chiara Fonio, Catarina Frois and Gemma Galdon Clavell
Authoritarian surveillance and its legacy in South-European societies: Greece, Italy, Spain, Portugal
This paper is a joint effort and a first attempt to critically and comparatively analyze past authoritarian surveillance and its legacy in four South European societies: Greece, Italy, Spain and Portugal. While Portugal and Spain had long-lasting dictatorships, Greece had a short military dictatorship but a prolonged post-war repressive police state; Italy had comparatively a short-term fascist regime back in the early twenties and a lasting post war democracy. Despite these and other significant differences in economic and political development, all these South-European societies share a relatively similar authoritarian past, and have gone through a similar Europeanization democratic process as members of the European Union (E.U.) with embedded democratic institutions. Hence, they are post-authoritarian surveillance societies, sharing a past authoritarian surveillance culture and similar surveillance trends and privacy protection policies as member-states of the E.U. Our socio-historical and cultural approach, which is mostly missing or neglected in the surveillance studies of northern countries, points out the significance of authoritarian surveillance operation and legacy to the understanding of current surveillance processes. The overall aim of this joint effort is to "open up" the debate, acknowledging the need for further comparative research.

Lorena Tarlion
Surveillance, classified information and human rights in post-authoritarian society
The intention in regards to this matter is the analysis of the state obligation:
- To prioritise the principle of loyalty in evidence administration, the weapons equality and the right to a fair trial, as told by the Human Rights European Convention and the jurisprudence CEDO, when documents that contain classified information represent evidence.
- To offer proper and sufficient security against abuse, because a secret surveillance system, whose purpose is to protect, for example, national security, motivated by the need to defend the democracy, creates the risk to undermine it or even destroy it.

Because the loyalty of evidence administration is one aspect of the evidence gathering process needed to have a legal sentence, honouring the human rights and the justice system, I consider that this principle is in close connection with that of the lawfulness in administering evidence, which means that, during the trial, to be administered only evidence stated in the law and by following the legal requirements. The classification of some documents, data, information obtained using various surveillance methods, which constitute evidence, and limiting or conditioning of access to these, has a direct impact on the above principles, leading to significant compatibility problems, undoubtedly influencing the judge's independence and impartiality.

Razvan Viorescu and Radu Chirita
How is Romanian Constitutional Court shaping the future of European data retention according to Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006?
Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks is without prejudice to the power of Member States to adopt legislative measures concerning the right of access to, and use of, data by national authorities, as designated by them. National entire implementing law no. 298/2008 ruled unconstitutional – thoroughgoing critique of data retention according to CC Decision no. 1258/08 October 2009 (Challenge to Arts 1 and 15 based on violation of constitutional and ECHR rights of privacy and freedom of expression). Under the Penal Procedure Code, content and comms data may be intercepted and retained for 6 months, pursuant to judicial authorisation based on suspicion of a specific crime. That is a justifiable exception from the rights to privacy and expression for the legitimate aim of preventing and detecting crime. "Continuous" retention of all data for fixed period of 6 months turns an exception into an "absolute rule". The positive rights to privacy and free expression lose their "prevailing role" and are instead "regulated in a negative manner". According to art 147 of the Romanian Constitution, the legal provisions on data retention are now suspended.

Ales Zavrsnik
Surveillance in Post-socialist Western Balkan Countries: from national security to big business?
The cultural bias of contemporary surveillance studies has been highly debated, e.g. in the light of an intercultural comparison conducted by Murukami Wood with the aim of deepening our understanding of the diversity of modern surveillance societies (in The 'Surveillance Society': Questions of History, Place and Culture, European Journal of Criminology, 6 (2), 2009) or in the light of French theory by Klauser (in 'Lost' Surveillance Studies, Surveillance & Society, 6 (1), 2009). The geographical limitation of the paper will thus try to fill this gap (or part of it) and supplement existing surveillance studies with insights from a part of Europe which has to date been unrepresented in the field. It will identify, analyse, evaluate and compare technically enhanced surveillance practices (TESPs) in countries within the territory of the ex-Yugoslavia (Western Balkan countries). Factors justifying the geographical focus of the project are the very rapid and profound political, economic, social and legal changes that marked the region over the last 20 years. These changes encompass, in particular, the transition to a capitalist market economy, the introduction of private property, denationalization and privatization, a reduction of social rights, greater unemployment, the fear of a powerful state, changes in crime and attitudes to it, the privatization of crime control, increasing prison populations, a failure to modernise the criminal justice system. These are some of the factors justifying the geographical focus of the paper and will be discussed in relation to particular TESPs in the region. The above-mentioned trends have not only influenced the attitudes towards specific surveillance practices and technologies, but also promoted particular *subjects* (actors) of surveillance (e.g. private actors of surveillance in video monitoring), *domains* of surveillance (e.g. flourishing surveillance in the domain of consumer surveillance that is less strictly regulated and conducted for target advertising, designing consumer portfolios, consumer segmentation, new product development and also consumer commodity), *justifications* of surveillance (e.g. business and profit oriented surveillance practices instead of public safety and national security driven surveillance) etc.

Open Session Papers

Timo Airaksinen
Open and closed surveillance
Closed surveillance is a continuum between Big Brother Surveillance (special closed surveillance) or Thingummy Surveillance (universal closed surveillance), in the following sense. BB (Orwell) is an agent who uses more or less well known methods and doodads to survey us citizens, that is my neighbors. TS on the contrary is everywhere and is conducted by invisible agencies with apparently unlimited power. An Open System is characterized by the slogan: "Survey your brethren; report all the deviations". An open network is created in which everyone surveys each other but without a center or a controlling power hub. This is the methodological framework and the question is: where are we going? Closed Surveillance is still here, and in an alarming manner the power of Thingummy Surveillance may increase. It is all secret. Some utopian theorists are suggesting that the Open System could be the main alternative in the future. I doubt it. As an example I will discuss the special role of the Secret Police, like the Stasi, in the contemporary world. Many apparently democratic states still contain a very real aspect of state terrorism because of such police. I say something on the motivation to nurture such state terrorism (security) and also on its abolition (liberty).

Thomas Allmer
A critical contribution to theoretical foundations of privacy studies
(1) Purpose: Although there is much public talk about privacy, it seems that there is no definite answer; rather, ambiguous concepts of what privacy is and what Indeed privacy in peril is. The overall aim of this paper is to clarify how privacy is defined in the academic literature, what the different concepts of privacy have in common, what distinguish them from one another, and what advantages and disadvantages such definitions have in order to clarify if there is a gap in the existing literature. (2) Approach/Theoretical Framework/Design/Methodology: This contribution constructs theoretically bounded typologies in order to systemize the listing literature of privacy studies and to analyse examples of privacy (threats). Therefore, it mainly is a theoretical approach combined with illustrative examples. (3) Findings: This paper contains a systematic discussion of the state of The art of privacy studies By establishing a typology of existing privacy definitions and discussing commonalties and differences. In this contribution, it is argued that the existing literature might be insufficient for studying privacy. (4) Originality/Value: In contrast, a critical notion of privacy and surveillance studies avoids pitfalls of the existing literature and strives for the development of theoretical and empirical research methods In order to focus on privacy in the context of domination, asymmetrical power relations, resource control, and social struggles. (5) Practical and Societal Implications: A critical contribution to privacy and surveillance studies wants to overcome surveillance threats as well as entrepreneurial privacy protection and privacy protection for other powerful actors in society in order to establish political processes and social transformations towards a participatory society.

Jonathan Bright
Reconsidering the economics of surveillant assemblage: the case of identity system convergence
Convergence is a central preoccupation of modern surveillance studies. The idea that once discrete surveillance systems in diverse sectors are beginning to join together is a recurring theme in the field, and is perhaps best captured in Kevin Haggerty and Richard Ericson's notion of the "surveillant assemblage". Yet despite the apparent popularity of the concept, theoretical explorations of the precise mechanics of assemblage have been rare. When exactly do assemblages emerge, and what motivates their construction? This article explores these questions, through reference to the construction of national electronic identification systems, which are becoming increasingly common throughout Europe. These systems aim to provide secure

mechanisms for electronic identification in a wide variety of public and private transactions, and hence "assemble" the identity functions of society into a single system. The argument defended is that the theory of assemblage is largely, if somewhat implicitly, based around the decreasing costs to personal information sharing implied by computerisation. However, whilst computerisation has certainly had an impact, many areas where these costs are *not* decreasing have been overlooked. In particular, the end user of these systems, frequently portrayed as relatively powerless, is actually in a strong position to affect business decisions about online identity management, and therefore the overall possibility for these types of assemblages to emerge.

Gema Galdon Clavell
CCTV in Spain. An empirical account of the deployment of video-surveillance in a Southern-European country
The use of video surveillance has been growing in scope and numbers over the last decades, with a steep progression in recent years. However, research on the national contexts that have driven such developments remain scarce and uneven, with most of the existing reports concentrating on Northern and Western Europe. This paper explores the situation of CCTV in Spain, its legal framework, shortcomings, public perceptions and specificity – such as a pre-9/11 concern for terrorism but its minimal impact on the justification for CCTV, a rights-based and *a priori* control of video surveillance devices and a deployment pattern that differs from those identified in the literature on CCTV at the Europe and global level. In providing an account on how Spain has joined the "surveillance society", it exposes a picture of unevenness, legal loopholes and resistance, and provides a first and unique overview of CCTV deployment in a Southern-European, post-authoritarian country.

John Guelke
Tension with the concept of privacy.
The current literature on privacy has a number of shortcomings. Many theories make impossible a satisfactory resolution of tensions between the value of privacy and other values. Many accounts ascribe implausibly strong normative protections to conduct in public places. Finally, the literature suffers from an 'individualist bias', frequently setting up an oversimplified tension between the individual benefits and societal costs. I propose an alternative theory of privacy, drawing on Scanlon's model of privacy in terms of 'laws and conventions' protecting zones or territories, and arguing for societal benefits of privacy, further drawing on comments of Nagel's. Norms of privacy, I argue, function partly to foster trust and cooperation for the wide range of interactions that make up an effective democratic social and political order. As the recent civic engagement literature makes clear, democracy is not just a matter of having certain institutions and freedoms, but requires substantive commitments from citizens to pursue a series of ongoing collaborative undertakings. Some of these undertakings require minimal cooperation for short periods of time, but others require long term, ongoing co-ordination. Successes in these various endeavours require trust among the participants, many of whom have different and sometimes incompatible beliefs and lifestyles.

Heta Aleksandra Gylling
Fear, surveillance and censorship
We are subjected to open and hidden surveillance. Traditionally the idea has been that in democratic societies, those responsible for safety and security, openly, not secretly watch and check potentially deceitful behaviour. Our identities are verified to safeguard us from behaviour which might harm individuals or public institutions. We do not want anyone to steal and use our "good name" and therefore many find it, for instance, highly ridiculous that some feel threatened by any security measures. They maintain that the innocent need not to worry, the measures taken are simply for preventing crime. Unfortunately innocence may have very little to do with the matter. Innocence is defined by the authorities who draw the boundaries of legally and morally

condemnable behaviour. Referring to the highly problematic concept of common or public good, they may try to justify secret surveillance of our behaviour and even expression of ideas. Authorities, who prefer security, want to maximize it at the expense of freedom and liberty. For them, privacy and freedom are over-rated and therefore they are willing to extend alleged "harmful" behaviour from actual activities to freedom of expression as well. But what counts as harmful freedom of expression in a democratic, pluralist society? Is it possible to find justifications for interference and secret surveillance? Or, should we, in the name of social stability, encourage people to self-censorship and openness so that secrecy regarding private matters would become a sign of moral or legal guilt? In my paper I will analyse varieties of fear and anxiety and their underlying causes as well as differences and similarities between surveillance and censorship.

Jesús M. Hermida and Alexandra Balahur
Moving into the cloud: Your data is everywhere, but where is it?
The era in which we live has been given many names. "Global village", "information society", "information age", and "knowledge society" are just a few of the terms that have been used, in an attempt to describe the deep changes that have occurred in the lives of societies and people worldwide as a result of the fast development of ICT technologies, the access to the Internet and its transformation into a social Web. For the times in which we live, information has become the main trading object. In this new context, the access to data, anywhere, at any time, is of crucial importance. More and more users are deeply involved in a process that globalizes data in order to make it accessible, sharable and usable everywhere. New applications are continuously emerging on the Web that not only allow people to share their personal data or experiences through the different social network sites (Facebook), but also offer free storage (Dropbox, Microsoft Skydrive) or even a complete operating system to work with (Google Chrome OS, Microsoft Office Online, EyeOS). Users move their data into these systems without knowing where they are (physically), who manages them (people, companies) or how many servers they manage. These systems compose the so-called "cloud" – an uncertain place that is not possible to reach. In order to take advantage of the benefits offered by universal data accessibility, users need to leave the responsibility of managing their data on their behalf to the cloud. In this way, many times unconsciously, they partly lose the control of their own information. In this paper, we will discuss on the advantages and disadvantages of using the services offered through "the cloud". We will present the opportunities, but also pitfalls related to data privacy in such services. The cloud should be seen as a tool with its benefits and risks. Users should be aware of them and conscious of the general process they are involved in. This will actually minimize the impact over their privacy and the use of their own personal data, while maintaining the benefits of having their information available at all times – an undeniable necessity in the society we live in.

André Jansson
Perceptions of surveillance: reflexivity and trust in a mediatized world (the case of Sweden)
There are still too few studies that have empirically tried to explain and thoroughly understand people's perceptions of 'surveillance society', and their modes of coping with mediated surveillance in everyday life. The aim of this paper, which is part of the ongoing research project *Secure Spaces: Media, Consumption and Social Surveillance* (funded by *Riksbankens Jubileumsfond*, Sweden) is to provide a 'middle range' social theorization, as well as an updated empirical account of how mediated surveillance practices are conceived and integrated with the social construction of identity, and thus also with the structuration of society at large. The analysis applies Giddens's perspective on the socialpsychological relationship between self and society, paying particular attention to the tension field between *reflexivity* and *trust*. Whereas the first part of the paper sets out this analytical framework, the second part presents the results from a national Swedish survey dealing with people's perceptions of integrity risks in relation to various forms of (potential) surveillance. The main argument is that the realm of social media nurtures an expanding culture of

interveillance which blurs the line between systemic and social trust, and thus calls for new, context specific modes of routinized reflexivity for coping with social uncertainty.

Anat Leibler
The science of population in a state of exception
In this paper I wish to discuss the difficulties of conceptualizing science-state connection when it comes to conflict zones. The conceptual sophistication that 'governmentality' offers those who deal with sites of knowledge production in the realm of the state is bounded by some limitations: While governmentality furnishes a wide range of studies of surveillance practices, it is limited when one comes to analyze the operation of these practices in countries with internal ethnic violent conflict. I will base my analysis on three cases of documenting individuals in Israel and the Occupied Territories: the 1948 census and population registration after the constitution of the new state of Israel; the 1967 census and population registration in the occupied territories right after the six-day war; the new law for biometric ID cards that eventually will be mandatory for all the citizens in Israel. These cases represent a shift from policing residents and citizens while crossing borders to a reality of living in ubiquitous borders.

Raluca Popa and Adina Diaconescu
The protection of private life and video surveillance -the Case of Romania
Video surveillance is necessary for the security of states but its use leads to an unduly negative effect on society supervised individuals' rights, especially the right to privacy.
In Romania, the operation to capture images and sounds is subject to supervision and control of the National Supervisory Authority for Personal Data Processing. Surveillance Authority's main object is to safeguard the rights and freedoms of individuals, in particular the right to privacy, family or private, in connection with the processing of personal data and the free movement of such data.
The supervisory authority has conducted a series of investigations in connection with the processing of video surveillance data from the office or as a result of referrals or receipt of complaints from people concerned.
Given the high impact of video surveillance in public places, investigations conducted by representatives of the Supervisory Authority pursued primarily systems installed in vehicles, banks, supermarkets, casinos, highways, schools.
Considering the cases found in the supervisory authority's practice and that in the Law no. 677/2001 on the protection of individuals with regard to the processing of personal data and free movement of such data there are no specific provisions regarding the processing of personal data by means of video surveillance, the authority is developing a resolution of the President of National Supervisory Authority, to regulate the processing of personal data for surveillance video.

Ian Tucker
Cybersurveillance technologies and everyday life
The post-9/11 world has seen a proliferation of forms of surveillance, both as a result of increased political needs for greater national and international security, and also due to 'new media' creating new technological forms of surveillance (e.g. cybersurveillance). Such advances result in increasing potential impacts on everyday living of forms of surveillance, for example from needing to allow more time to get through airport security to consideration of the amount of personal information is made 'public' through engaging with new social media. Crucial to how people attempt to make sense of living in surveillance societies is their knowledge and experience of the range of technologies that can act as surveillance. People's experiences often revolve around notions of privacy, which can be understood not as a quantifiable entity (something people have more of less of), but as produced as a relational product between organisational activity and the localised practices of everyday living (Haggerty & Ericson, 2006). The aim of this paper is to draw attention to and analyse the impact of post-9/11 surveillance technologies on everyday life,

particularly the role of forms of cybersurveillance that have proliferated in the past ten years. The impact of internet technology in creating new modes of connecting with others has been well versed (Abbate, 1999; Aune, 1996; Barabasi, 2002). Crucial to this discussion is the role of the technology itself, as it brings with it new abilities that alter prior forms of communication, for instance the facility of storing and recording the digitalised activity that it allows. The technology itself acts as a *mediator*, and moreover a new form of mediation that brings with it a raft of changes to the kind of forms of communication that are possible (e.g. instant dialogue with people and organisations in countries across the world). The rise of internet-based activities has contributed to an increasing 'informationalisation' of people (Bogard, 1996), through providing ever more ways of connecting with other people and organisations (e.g. banks). This proliferation of technologies of surveillance has led some to utilise Deleuze's notion of 'assemblage' rather than the previously dominant Foucauldian 'panopticon' model of surveillance. This paper draws attention to the kinds of 'technologies of the self' that are possible within contemporary surveillance societies. This draws on Foucault's later work around analysing the activity of 'organisational power', and its connections to people's localised practices. Central to this is the role of privacy as a fluid concept continually subject to potential threat and alteration by the proliferating forms of cybersurveillance. This results in increasingly fuzzy boundaries between the flesh and blood of bodies (which are a traditional constituent of the self) and our 'data-selves' formed through interaction (knowingly and unknowingly) with cybersurveillance technologies (Fuller, 2005). In summary the paper is focused on how internet technologies act as forms of cybersurveillance to produce new modes of experience, which themselves challenge and potentially recalibrate our notions of self. This is particularly relevant to notions of privacy – oft used in debates about use of personal data by organisations – which are themselves exposed to shifting understandings and formulations. This paper draws on data from a wider project involving semi-structured interviews with members of the public living in a major UK city. The interviews focused on interviewees' knowledge and experience of surveillance, with the objective of highlighting some of the ways that it impacts on everyday life.

Susanne Wigorts Yngvesson
Security above all? Moral implications and criteria of surveillance in the workplace
In workplace ethics, particular criteria are used to regulate and distinguish "private sphere" from "workplace sphere". For security or efficiency reasons surveillance are being motivated. But an employee also has a right to privacy. So, on what grounds can intrusion of privacy be justified? Surveillance can be interpreted both as an instrument of security and as an intrusion of the "private sphere". The terminology of private and public is not very useful here for finding criteria of moral dilemmas. There is a tendency that people seem to want surveillance to be a protection from "outside dangers", but they are not as keen about being surveilled in their daily life activities. Should preferences guide all decisions about surveillance or are there other interests to consider? What criteria should guide decisions about surveillance? In this paper I will discuss: (a) what moral principles that should guide judgements about evaluating surveillance practices in the workplaces, and (b) what criteria that shows when intrusions of an employee are justified in relation to surveillance.

European Research Project Presentations

Thomas Allmer
Social networking sites in the surveillance society
Social networking sites (SNS) are Internet-based platforms that allow users to construct profiles, establish displayed connections with other users, and that support various forms of online communication. Examples are studiVZ, MySpace, or Facebook. The overall aim of this research project is to study electronic surveillance on social networking sites that are used by Austrian students. The specific research questions are: (1) How important are the topics data surveillance and privacy in discussions by SNS users? Which arguments do they use for arguing that they disagree or agree with surveillance on SNS? (2) Which major advantages and disadvantages of social networking platforms do Austrian students see? What is the role of surveillance and privacy in this context? (3) Are knowledge and attitude towards surveillance and privacy of Austrian students and their information behaviour on social networking platforms connected? The research methods employed are qualitative interviewing (for research question 1) and quantitative and qualitative surveys (for research questions 2 and 3). Theoretical foundations of surveillance and privacy will be systematically elaborated. The project will contribute to a political economy of surveillance and privacy. In this context, interviews with students about their understandings of privacy and surveillance on SNS and their attitudes towards these interwoven issues will be conducted. A survey that is focusing on students from 18 major Austrian universities as potential respondents will be carried out. We will analyse which major advantages and disadvantages students see in SNS. We will also analyse which role surveillance and privacy play in the context of the advantages and disadvantages that students perceive, how large their knowledge of surveillance is in general (surveillance knowledge index), which attitudes they have towards surveillance (surveillance critique index) and privacy, how much knowledge they have about concrete SNS that are used in Austria, and their information behaviour (advertising settings, privacy settings, etc) about specific SNS. These variables will be correlated in order to find out if and how the surveillance and privacy variables and SNS usage are causally connected. It will be discussed how perceived surveillance risks can be reduced.
Institutional affiliation: Unified Theory of Information (UTI) Research Group
Funding agency: Austrian Science Fund (FWF)
Contact details: http://www.sns3.uti.at
Researchers involved: Christian Fuchs (Project Coordinator); Thomas Allmer (Research Associate); Verena Kreilinger (Research Associate); Sebastian Sevignani (Research Associate)

Miyase Christensen and André Jansson
Secure spaces: media, consumption and social surveillance
As people strive to become more flexible, connected and mobile through the use of new media, they also become subject to various forms of surveillance. While new media enable geographically extended experiences and deepened senses of social community, security and control, they also tie the individual to abstract systems that enable tracking and monitoring of e g consumption habits, mobility and private interests. These new media are also a central force within the accelerating consumer culture. Against this background the aim of the project is to map out and provide a deeper understanding of how people today handle various media forms in order to strengthen their sense of security and control, and to clarify how these patterns and experiences are related to overarching structures in contemporary society. The analyses consist of a combination of survey (the SOM Institute) and qualitative interviews.
Project leader: André Jansson, Karlstad University.
Co-investigator: Miyase Christensen, Karlstad University
Funding agency: *Riksbankens Jubileumsfond* 2009-2011.
Website: http://www.kau.se/en/humanit/research/secure-spaces-media-consumption-and-social-surveillance

John Guelke
The DETECTOR Project
The DETECTER project is funded under the European Framework Seven Securities programme. Most research funded under this programme is concerned primarily with developing new technology or applying existing technology to current security problems. Our project, by contrast, concerns the ethical and legal norms of the use of detection technology. The project is carrying out original research on hot topics, like counter-terrorism data mining programmes, monitoring of Internet activity and the role of technology in pre entry screening of foreign migrants. It also is making contributions to debates on how privacy should be viewed in the counter-terrorism context from the perspective of both law and ethics. The project hosts 6 meetings under Chatham House rules between technology developers, many drawn from Framework 6 and Framework 7 funded projects, and end users in counter-terrorism policing and intelligence. These meetings have succeeded in providing a forum for robust discussion of the ethical dilemmas involved in developing this technology, the needs of counter-terrorism professionals, and the dangers of excessive confidence in technology. The project is lead by the University of Birmingham, and the partners include the European University Institute, the University of Zurich, the Raoul Wallenberg Institute in Lund, the University of Oslo, Abo Academy University and the Danish Institute for Human Rights.
Project Leader: Prof. Tom Sorell
Funding Agency: European Commission FP7
Website: http://www.detecter.bham.ac.uk/

Michael Nagenborg and Ivan Szekely
Ethical issues of emerging ICT applications (ETICA)
In the first part of the presentation an overview of the framework and research findings of the ETICA project will be presented. ETICA, a major European research project involving 12 partners across Europe and supported by the EU's Framework 7 Programme, was launched in 2009 with the aim of identifying emerging technologies likely to be realized in the next 10–15 years, and their ethical implications. This was followed by the ranking and evaluation of the identified ethical issues and the analysis of governance structures within which ethical issues of emerging technologies would be dealt with. Following a series of professional discussions, workshops, conferences and policy briefings – including the presentation of ETICA in the European Parliament – the research consortium is now planning to present its recommendations to the EU Commission on emerging and future technologies and their related ethical issues. In the second part the findings of the evaluation of emerging technologies in the area of legal implications will be presented. The analysis was based on the premise that the law is supposed to invoke moral principles. It included an empirical research conducted in the whole legal corpus of the EU and found that the legal implications of emerging technologies have attracted only a minimal legislative attention in the competent bodies of the EU. The evaluation provided a systemic approach towards transmitting ethical norms to the application of emerging technologies through legal regulation, and formulated detailed recommendations in various areas of such technologies.
Researchers: Michael Nagenborg and Ivan Szekely
Funding agency: European Commission, 7th Framework Programme
Website: http://moriarty.tech.dmu.ac.uk:8080/

Michael Nagenborg
Security ethics: BaSiD, MuViT, and KRETA
The Research Group on Security Ethics at the International Centre for Ethics in the Sciences and Humanities (IZEW, University of Tübingen, Germany) has been established in 2007. The Research Group serves as an interdisciplinary platform for different research projects. Most of the projects are concerned with ethical issues of security technologies, and most of the projects are funded

within the Research Programme for civil security of the German Federal Ministry of Education and Research (BMBF). After giving a short overview of the IZEW and the German Research programme for civil security, three current projects will be highlighted. BaSiD (= Barometer Security in Germany) is developing an instrument to measure objective and subjective (in)securities in Germany. MuViT (= "Pattern Recognition and Video Tracking") addresses the sociological, social psychological, legal, and ethical aspects of so-called 'intelligent video surveillance.' Finally, KRETA is an interdisciplinary project on the interplay of security, technology, and 'deviant bodies.' This interplay is assessed in terms of justice as the guiding normative principle.
Researchers: Prof. Dr. Regina Ammicht Quinn (Project Lead; theology), Andreas Wolkenstein (Researchgroup Coordinator; MuViT, KRETA; philosophy), Dr. Michael Nagenborg (BaSiD, KRETA; philosophy) and others.
Funding agency: German Federal Ministry of Education and Research (BMBF)
Website: http://www.izew.uni-tuebingen.de/ or
http://www.uni-tuebingen.de/en/facilities/international-centre-for-ethics-in-the-sciences-and-humanities.html

Jason Pridmore
DigIDeas: Social and Ethical Aspects of Digital Identities. Towards a Value Sensitive Identity Management
Digitisation and automation processes pervade virtually all aspects and domains of society. The need for reliable identification and the verification of identity has led to an increasing reliance on information technologies to provide for an automated recognition of persons. At the same time, the growth of digital communications, interactions, and transactions has produced vast amounts of personal data that can be linked and connected to track individuals and produce personal profiles that are unprecedented in detail, availability and durability. Alongside these possibilities is the popularity of on-line identity construction through personal websites, social networking sites, (micro)blogs, online communities etc., where people voluntarily present detailed textual and visual accounts of their lives to mass audiences. Taken together, and partly intersecting, these developments constitute a set of remarkable new phenomena. The DigIDeas project examines the ways in which new identification technologies and digital media mediate and transform identities, connecting with the notion of 'identity' as a key concept in contemporary social theory, and in current conceptualisations of the relation between technology and society. Drawing on resources from social and constructivist studies of science and technology, surveillance studies, and philosophy of technology, the project looks at six empirical domains of identity management. These are referred to as Civic and Secure, Suspect and Ubiquitous, and Profitable and Personal Identities. The project will contribute to both international academic debates on these issues and aid in developing more value sensitive policies and technical innovations.
Researchers: Coordinated by Irma van der Ploeg
Funding agency: European Research Council Starting Grant
Website: www.digideas.nl

Bence Ságvári
EU KIDS ONLINE II.
Between 2009 and 2011, EU Kids Online II conducted original empirical research across member states with national samples of children aged 9-16 years old and their parents. The aim was to produce a rigorous, cross-nationally comparative quantitative evidence base regarding internet use across Europe. Online risks high on public, research and policy agendas include exposure to inappropriate content, unwelcome contact, and, attracting growing attention, inappropriate conduct by children themselves (i.e. abuse of privacy). Children's intensifying use of social media and other services/technologies brings new phenomena in the topics of surveillance and privacy. The presentation briefly summarizes the main findings of the empirical research and provides important insights on children's and parents' perceptions and practices regarding online risk and safety.
Head of Research: Sonia Livingstone, London School of Economics
Head of Hungarian research team: Bence Ságvári, ITHAKA Research and Consulting
Funding: EU Safer Internet Program
Website: http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EUKidsII%20(2009-11)/home.aspx

Doctoral School Presentations

Bright, Jon
Security (in) Formation: Identification and Personal Information in the 21st Century
Constructivism in international relations has so far focussed primarily on intention: how states decide upon courses of action, and how these courses of action are legitimated. Constructivism in science and technology studies, while using many of the same theoretical starting points, has been directed more towards the construction of results: how are technologies created, and how are facts established as truths? Despite shared premises, there has been relatively little dialogue between these two variants of constructivism: this thesis seeks to fill this gap. Its focus is on the role of personal information in national security, and particularly on the construction of the technology required to personalise information: identification systems. Following Latour, I take a thick constructivist approach to the creation of these systems. The reasons for the construction of identification technology are held to be manufactured in the same way as the technology itself, through a social and political process where meanings are constantly contested. The central argument of the thesis is that while the construction of "security", broadly defined, has proved an important motivator in the creation of national identification systems, these security needs have also hampered the development of these systems through the way identification for security is constructed.

Filipe Santos
The 'CSI effect': Impacts of popular culture on representations about DNA evidence
The purpose of this presentation will be to provide a background for the discussion of the doctoral research project, focusing on the importance of DNA evidence, its dissemination in the media and its possible effects, and the Portuguese context's relevance for the research. The use of DNA technology in the criminal justice system has, according to some authors, introduced a new paradigm in forensic science. Simultaneously, the forensic science fiction TV series genre like *CSI* has contributed to the dissemination of information about forensic science techniques and their association with images of neutrality, certainty and objectivity, as well as characterizations of criminal investigations as being quick and effective. In the adversarial context, the CSI effect emerges as a possible explanation for a transformation in the way scientific evidence is perceived and evaluated by the general public and juries, but also in the way it is managed by judicial actors, such as lawyers and prosecutors. However, in Portugal, the research about the influence of fictional narratives on the representations of forensic genetics is still in its inception. This doctoral research project aims to provide an original contribution on a national and international level, insofar as, on the one hand, it intends to assess the manifestation of a CSI effect within a inquisitorial justice system and, on the other hand, it will attempt to understand the impacts and expectations associated to the popularization of forensic genetics in the media coverage of criminal cases as well as on the actors of the criminal justice system.

Vlad Niculescu Dinca
Policing in a world of ubiquitous identification
Within the DigIDeas project, this project examines the ethical and social issues at the intersection between new developments towards ubiquitous identification (Van der Ploeg 2008) and policing practices, aiming to contribute to a value sensitive design and management of digital identities (Nissenbaum 1998; Friedman 2006; Van den Hoven 2007). The project is grounded empirically in an open set of case studies that may include smart video surveillance systems (video analytics with pattern recognition), GIS in the context of policing and criminal justice, and different (RFID) applications within the 'internet of things', storing, classifying, geo-coding, aggregating and mining personally identifiable data in increasingly interconnected identity management systems. Such developments are more than likely to effect societal change, yet they are themselves shaped by societal processes and values (Hildebrandt and Gurtwith 2008). The research takes a general STS

approach (Science and Technology Studies), including concepts from Actor Network Theory (Akrich 1992; Latour 1987, 1988), surveillance studies (Foucault 1977; Deleuze 1992; Haggerty K. and R. Ericson 2000; Lyon 2003; Norris Clive and Armstrong 1999), philosophy of technology (Bijker 1995; Brey 2000) and identity theories (Bowker & S.L. Star 1999).

Panagiotis Kitsos
The protection of personal data and privacy in the electronic communications sector: The case of Greek law 3471/2006 and the transposition of Directive 2002/58/EC.
The primary goal of this thesis is to validate the transposition Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector as amended by directives 2006/24/EC (Data Retention Directive) and 2009/136/EC (Citizens Rights Directive) in Greek law. The research is conducted through the presentation and analysis of the existing legislative framework on personal data protection, at national and international level. In the first part a conceptual analysis on privacy and personal data is attempted with references to European and American philosophical and legal theory as well as in case law. In the second Part an introduction to the subject is made with the presentation of the generational development of Data Protection in Europe from the so-called "first generation" regulations to the current national and E.U legislative initiatives. A comparative analysis of the Greek Law as opposed to Directive 2002/58/EC and the evaluation of the degree of the effectiveness on the protection of personal data and privacy in Greece follows. As a conclusion the thesis emphasizes the growing need for a strong legal approach to data protection in the light of the emerging technologies and confirms that under the existing international regulatory environment Greece has built a rather strong legislative framework regarding the protection of personal data.

Ask Risom Bøge
Surveillance and the body
The body is becoming targeted as a source of surveillance data. Biometric surveillance technologies such as fingerprint scanners, biometric passports and video cameras with facial recognition programs are increasingly utilized in the fights against crime, illegal immigration and terror. The epitome of this trend, and the context of my research, is the proliferation and constant expansions of police controlled DNA databases in the European Union and USA. DNA surveillance distinguishes itself from all other biometric techniques, in that it operates on the innermost and most personal patterns of our bodies. As such, more than 80,000 DNA profiles from crime scenes, suspects, and convicts are subjected daily to virtual control, in the rapidly growing Danish National DNA Database. In my research, I focus on the uses of DNA technologies by the Danish police in a combined historic and ethnographic perspective. Based on records, newspaper articles, interviews and observations I investigate the development of DNA methods and their implementation and use in police practices. Theoretically, the PhD interprets oligoptic surveillance (Latour 2005) through concepts affiliated with post-ANT (Law & Hassard 1999) and social anthropology (Strathern 1991). Collectively, these positions offer an interesting theoretical framework, in which DNA-based surveillance may be understood as being composed of fragile connections and situated visualizations.

Philip Schütz
Theoretical and methodological concepts of analysing data protection authorities in a comparative perspective
This dissertation project aims for a comparative analysis of data protection authorities (DPAs) in EU Member States. Since the EU Data Protection Directive 95/46/EC was adopted in 1995, the set up of DPAs on a national level has been mandatory for the Member States. However, given the fact that there is latitude in the implementation process of European legislation, central features and assigned roles of DPAs vary greatly. Thus, the thesis focuses on the following questions: Which differences in the set up of DPAs can be identified and what are the causes for the

variations? Within the next three years five country case studies will be conducted. At the moment the dissertation project that has just started deals with the operationalisation of formal as well as informal aspects of DPAs' independence, drawing on elements of regulation theory such as the concept of the *regulatory state* and independent regulatory agencies (IRAs). While outlining the most important features of the theoretical approaches, two studies are presented that attempt to measure independence of IRAs. Eventually, the independence of German DPAs, which will serve as a starting point of one of the five case studies, is discussed