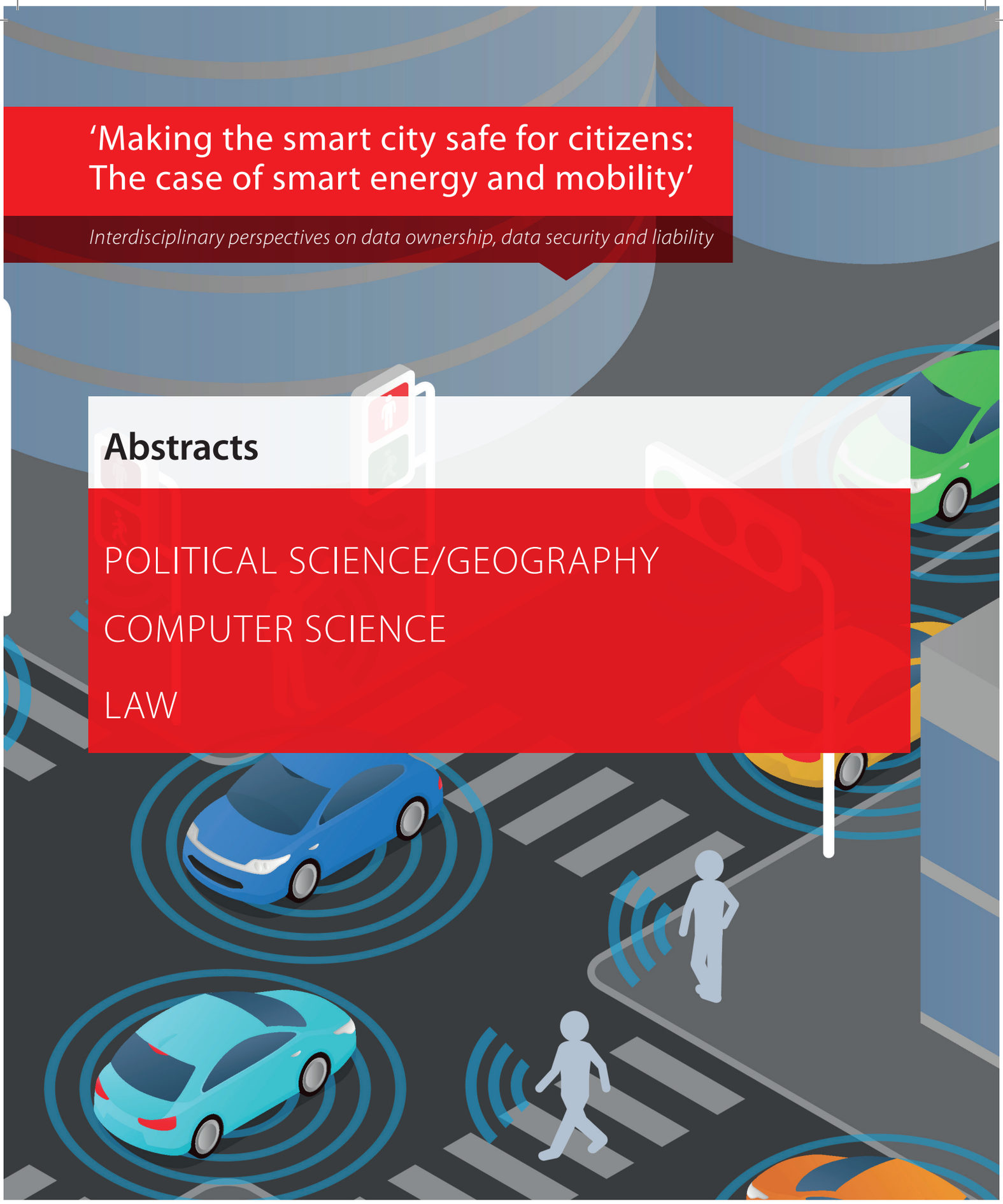
‘Making the smart city safe for citizens: The case of smart energy and mobility’

Interdisciplinary perspectives on data ownership, data security and liability



Abstracts

POLITICAL SCIENCE/GEOGRAPHY

COMPUTER SCIENCE

LAW

BISS

Open Universiteit
www.ou.nl

Political Science/Geography

DAUM, TIMO

Data-driven transport in the city: who will own it, who will govern it?

Prof. Timo Daum, SRH-Hochschule Berlin, BTK-Hamburg & Universität Hildesheim, Germany

Abstract

The leading global data companies from California are attempting to establish platform capitalism in the sphere of mobility, in order to successfully implement their data extractivist business models in this field. IT giants like Google, Uber and Tesla are trying to establish a new form of transport, shifting from privately owned, combustion-engine powered, humanly steered cars towards an autonomous network-service, where algorithms and data play a key role. Uber has just announced their aim to make privately owned cars obsolete and replace public transport with its own ride-sharing-model – both in one hit.

MOIA, a Volkswagen AG enterprise, is currently attempting to enter the ride-sharing market in some German cities, claiming to act as a "social movement company". It advertises itself as a greener and smarter alternative, aiming at reducing congestion and lower prices. They follow the platform model of data ownership and algorithmic control. Deutsche Bahn AG on the other hand is currently experimenting with autonomous shuttle services to cover the last mile in passenger transportation. The comparison of the two test-runs will deliver a set of key indicators for the usefulness of the service from the user's perspective.

Key questions are: Who owns the data? Which goals are implemented in the algorithms? Does the service complement existing public transport or does it rather compete with it? Does it effectively replace individual motorized traffic? Are there mechanisms to push towards a greener, more environmental friendly mobility mix or not? The paper concludes that it's time to realize that the battle over sovereignty in the future city is about data, and who processes them, and about algorithms, and who implements their logic, their goals and mechanisms.

HAGGART, BLAYNE & SPICER, ZACHARY

Infrastructure, smart cities and the knowledge economy - the case of Sidewalk Labs and Waterfront Toronto

Assoc. Prof. dr. Blayne Haggart, University of Duisburg-Essen, Germany, and Brock University, Ontario, Canada
(dr. Zachary Spicer, University of Toronto, Canada)

Abstract

Sidewalk Lab's recently announced Quayside project in Toronto, Canada, offers a clear demonstration of how the spread of information technologies is beginning to shape cities' core governance functions. In October 2017, Waterfront Toronto, the tri-governmental agency (representing the Governments of Canada, the Province of Ontario, and the City of Toronto) responsible for the Toronto waterfront, announced that Sidewalk Labs, a subsidiary of Google's parent company Alphabet, would co- pilot a redevelopment of 12 acres of Toronto's south-eastern waterfront. The plan proposes turning an industrial area into one of the world's first purposefully designed "smart" communities, with sensors embedded throughout to monitor and adjust service and resource levels depending on resident use.

How should citizens and government officials evaluate such projects? Are traditional approaches to infrastructure development sufficient? Do policy-makers and the public have enough information about data management and privacy to properly evaluate and regulate such projects?

This paper proposes a theoretical and methodological framework for properly analyzing issues of economic development that captures the rising relative importance of data and intellectual property in projects such as Quayside. Based on the work of International Political Economy scholar Susan Strange, and understandings of knowledge derived from scholars of the sociology of knowledge, it emphasizes that changes in the dominant means by which economic wealth and political power are produced requires new means of analyzing and regulating both the economy and society in general. Such changes also require recognizing that governments have a key role in setting the framework governing how knowledge (which includes data and intellectual property) is to be created, disseminated and used, and, most importantly, in whose interest. If policymakers and citizens fail to appreciate the importance of these changes – for example, thinking of economic development in terms of physical-infrastructure development rather than as a means for data capturing and profiteering – they run the risk of sleepwalking into allowing non-state actors to implement sub-optimal, self-interested regulatory frameworks and projects that have the potential to cause great harm to society at large.

This paper applies our theoretical framework to the Sidewalk Labs proposal to illustrate how it can illuminate data/knowledge-specific blind sports that would otherwise be underappreciated by more traditional approaches. It then proposes a framework that policymakers at all levels can use to "ask the right questions" regarding "Smart City"-type developments and other forms of data- or knowledge-driven policy planning.

OELS, ANGELA

When NGOs run online campaigns on environmental issues: A theory-based critique drawing on Habermas and Foucault

PD dr. Angela Oels, OU Netherlands

Abstract

The Australian (left-wing) non-governmental organization (NGO) GetUp! tried to stop the re-election of a selected number of racist and climate-sceptic Members of Parliament (MPs) using big data and social media, mostly Facebook. Is this a welcome success story of how interest groups use the digital age to their advantage? Or is it voter manipulation and a threat to liberal democracy? Different social milieus respond to different ways of being addressed. Research on product marketing and placement has built on these insights for a long time. Digitalisation is now offering tools that are able to target subjects even better – with success as the Australian case shows. While this is certainly effective, there are also problematic aspects of social media campaigning, which I will discuss drawing on political theory. For the proponents of liberal democracy like Habermas, it is problematic that many sub-publics are addressed in a specific way. This contributes to a growing polarization and fragmentation of society living in parallel universes. Habermasians would ask where the spaces are for deliberation of a 'general public' that could lead to a 'general will' or shared ideas about the common good.

From a Foucaultian perspective, there is no such thing as a pre-existing 'free voter' who could be manipulated. Instead, voters are always already inscribed in certain dominant discourses and their social identity is shaped by these discourses. For Foucaultians, it is problematic that digital and social media show personalized campaign ads and search results, thereby reinforcing existing power relations and notions of who we already 'are'. Foucault's idea of emancipation was to resist who we are supposed to be. This of course requires a willingness to break out of the echo-chamber. Giving individuals access to alternative types of information, outside the range of who they are supposed to be, is an important precondition for running a campaign that has emancipatory qualities.

Political Science/Geography

REHAK, RAINER

General conditions for a safe smart city: Two necessary techno-political factors for safe and secure networked systems

Rainer Rehak, Weizenbaum-Institute for the Networked Society, Germany

Abstract

Regardless of the actual use case of any given smart city software system, properly implemented IT security – confidentiality, integrity and availability – is the basis for safe and expectable systems. This is even more so in a highly interconnected and networked setting which opens up large attack surfaces as typically seen in modern smart city infrastructure components. Although many approaches can improve the security of individual systems, the overall IT security situation is very worrisome and systematically bad. Using two examples of the recent IT security history – the KrebsOnSecurity DDoS incident of 2016 and the Wannacry worm of 2017 – I will argue for two major conditions that have to be met before any meaningful approach to making the smart city safe for citizens can be taken. Firstly, a digital society living in smart cities cannot proceed without general software liability anymore. One of the biggest threats to networked systems does not come from powerful specialized attack equipment but from small consumer IoT devices with usually insecure software. Those devices – from smart TVs to security webcams – rarely receive proper software updates nor are they generally of high software quality. If we want to take the notion of a networked society seriously, we have to extend our understanding of IT security from looking at one system only to looking and regulating the whole network of systems. The other major factor hindering generally improved IT security is government hacking in the form of direct or indirect (contracted) vulnerability stockpiling, instead of unconditional responsible disclosure obligations for all actors. As powerfully demonstrated by the Wannacry worm of 2017 – based on the stockpiled vulnerability 'eternal blue' from the National Security Agency (NSA), infecting and sabotaging infrastructure such as train systems, hospital networks or internet providers globally resulted in damages worth around US$4 billion and hospitals having to close. Keeping vulnerabilities open should not be possible for governments.

Especially governments, by their sheer financial power, are strengthening and sometimes even creating grey markets for software vulnerabilities and therefore contribute to global IT insecurity.

Only with those two techno-political changes the necessary systematic improvement of IT security in networked systems can be achieved to make a smart city truly safe for citizens.

REIA, JHESSICA

Who Owns our Data? Regulation, social participation, and privacy issues in Brazilian smart cities

dr. Jhessica Reia, FGV Law School, Brazil

Abstract

The Smart City formula has gained traction in academia, business, and government to describe cities that, on the one hand, are increasingly composed of and monitored by pervasive and ubiquitous computing and, on the other, are striving to restructure their economy and governance based on innovation, creativity and entrepreneurship. This tendency received the attention of those producing and utilizing data to monitor, regulate, profit from, and make sense of the urbanization process in both developed and developing countries.

In such context, the hype and hope of big data are fostering a transformation in the knowledge and governance of cities, since it provides much more sophisticated, wider-scale, real-time understanding, and control of urban planning for local governments. However, many smart city initiatives have failed to go beyond high-tech marketing rhetoric and gone on to improve everyday life conditions for all citizens. While the uses of these systems in Brazil are quite recent, they already raise concerns about human rights, inequality, poor systemic governance, or biased urban planning agendas. Ultimately, Smart City initiatives based on big data techniques of a personal data mass collection might also produce or deepen current social, cultural and economic inequalities, and produce discrimination, especially in the Global South.

Following the steps of the EU GDPR, Brazil has just approved, after years of public debate, its first General Data Protection Law—which will probably change the data governance of such initiatives. Having this multifaceted context in mind, the primary goal of this work is to present the main findings of a research project which aimed to analyze how the three Brazilian cities ranked as "smartest"—Rio de Janeiro, São Paulo, and Curitiba—are dealing with challenges of data ownership/governance. We will focus on privacy, social participation, and regulatory issues. Based on qualitative in-depth semi-structured interviews with key stakeholders (academia, companies, municipalities, civil society), participant observation in the largest smart cities forum and exhibitions in the country, and evaluation of current legislative and regulatory frameworks, the research aims to help shed light on current implementation of smart cities initiatives in Brazil. This research is part of a larger project on discrimination and data control in smart cities funded by the Open Society Foundations and developed at the Center for Technology and Society at FGV.

Political Science/Geography

STIFTER, EDITH

Smart city as a tool for control? The case of China

Edith Stifter, University of Vienna, Austria

Abstract

In Europe, the concept of a Smart City is understood as a governance tool that benefits the environment and citizens. It holds the promise for a better future in a smarter city. Yet, can Smart City also be used as a tool of social and political control, or even be designed as such in the first place?

China is leading in smart city development - at the beginning of this year, Deloitte reported that out of 1,000 smart city pilots worldwide 500 are located in China. At the same time, China is developing the Social Credit System (SCS), a government-scheme which will be fully developed until 2020 and whose exact scope and design is yet unknown. At its core, however, it is a personal rating system for citizens and companies that uses the merger of information from different domains—including transportation, legal, and commercial data—and public reputations to create a "culture of honesty". The SCS has stirred much debate in policy and public circles due to its apparent intent for technologically empowered social and political control. Recently, an Australian report claimed that the SCS has implications beyond the Chinese border.

A number of indications suggest that the development of smart city and the SCS are technologically and ideologically interwoven. For example, in the city of Hangzhou, a significant reduction of pollution and a better flow of traffic have been achieved with the Alibaba City Brain. Yet, Hangzhou is named as one of the 12 leading pilot areas for the development of the SCS. Is the case of Hangzhou a pure coincidence or are the smart city and the social credit system interwoven, technological and ideological?

Drawing on documents and plans from the Chinese governments, documents from international organizations (e.g. UNIDO), as well as Chinese and international media reporting this paper will provide a short chronology and a mapping of existing Smart City and SCS pilots. It will attempt to answer the following questions: to what extent are Smart City and SCS interdependent? Can Smart City be a vector for the export of the SCS? How is China influencing the definition and practical implementation of the Smart City concept?

WAHYUDDIN, YASSER

The role of Lyon as vector of climate-energy politics: The governance of Smart Electric Lyon toward energetic transition tools

Yasser Wahyuddin, Laboratory EVS-RIVES, ENTPE, University of Lyon, France

Abstract

EDF developed "Linky Smart Meter" as the core material of France Smart Grid policies. The embedded features of Linky were initially aimed at providing the citizen's awareness in view of empowerment and to better manage the daily consumption that corresponds to the actual needs, the possibility to avoid the peak times, and to be informed in real time of dynamic-pricing offers. Linky also plays as terminal for a rapid data stream from households/individual consumption in a real-time basis, creating individual "datafication" processes at the same time (Kitchin, 2014, Lupton, 2016, Mayer-Shonberger, 2017). Its first installation began in 2008-2009 where 270,000 units of Linky were installed in Lyon and Loire.

Political Science/Geography

EDF seemed to gain momentum as the leading promotor of France's Smart Grid since Linky is recognized as a smart city element. In 2012, EDF launched Smart Electric Lyon (SEL) project as a research and development program based on Linky under the banner of "Smart City." The SEL was formatted as a collaborative-platform gathering affiliated technology information, and communication (TIC) and electricity-industries companies, to extract the economy added-value upon the massive quantity of data generated by Linky.

Since then, Smart Grid program in France are demonstrated as a subcategory of Smart City. While in practice, the cities are the key points supporting Smart Grid innovation (Lecler et al., 2015). Facing the emerging technology penetration such as Smart City, the cities are vulnerable and being at risk on falling on the bottom line among multi-level actors. Numbers of pioneer analysis on Smart Cities were showing pessimistic signs on how cities could resist to the omnipresence of the new actors and new topics that presumably would cannibalize certain traditional city systems.

However, through the example of SEL, we singled out that the Lyon Metropolis holds a vital role at orienting the governance of industrial Smart City programs to associate its projects to Lyon's climate-energy plans. We identified a transformation of SEL that was initially designed as a Smart City project to become an instrument of Lyon's energetic transition. Our findings on SEL provide an essential proof to rethink the political role of the city. Under the grand coalition of multi-level actors with heterogeneous political-economy interests, Lyon managed to federate the governance of the smart City ecosystems in accordance to its climate-energy policy plan. We would like to address our argument to the actual critic on the phenomena of Smart City, stating the city as merely as the object of TIC market.

Computer science

FORMOLO, DANIEL

Simulating emergency communication for multicultural crowds with an agent-based model

dr. Daniel Formolo, Vrij University, Netherlands

Abstract

In this research, the effects of culture, cognitions, and emotions on crisis management and prevention are analysed. An agent-based crowd evacuation simulation model was created, named IMPACT, to study the evacuation process. The IMPACT model was validated against data from an evacuation drill using the existing EXODUS evacuation model. Results show that on all measures, the IMPACT model is within or close to the prescribed boundaries, thereby establishing its validity. Structured simulations with the validated model revealed important findings, including: the effect of doors as bottlenecks, social contagion and trained staff speeding up evacuation time, falling behaviour not affecting evacuation time significantly, and travelling in groups being more beneficial for evacuation time than travelling alone. This research has important practical applications for crowd management professionals and risk assessors.

HOLLEKAMP, THOMAS

Data security as a conceptual prerequisite for smart cities

Thomas Hollekamp, University of Bonn, Germany

Abstract

The topics smart city and data security are gaining worldwide interest in academia, society and economy. Smart city measures might solve environmental and energy related challenges in urban areas, but they will bring new challenges regarding data security and data protection due to the variety of processed data affecting critical infrastructures as well as personal privacy. The master thesis aims to give an interdisciplinary overview of security related problems in smart cities.

The research questions are: What are the new, specific problem areas in smart cities?
How can the data flow in smart cities be modelled?
How do tailored tools and measures for data security look like?

Henri Lefebvre's and David Harvey's right to the city approach frames the theoretical background. Especially smart city measures tend to exacerbate social inequality (digital divide), increase surveillance and dataveillance capabilities and therefore raise issues of data security, sovereignty, and privacy. At the same time, smart technologies offer opportunities for transparency and participation. Citizens should be actively engaged in smart city strategies, to prevent the corporatisation of city governance and a technological lock-in, as Rob Kitchin calls it.

A three-stage systematic literature review was conducted, to first get an overview of the general academic smart city discourse. Second, publications with regard to technical reference models of smart cities were analysed to develop a schematic smart city architecture model. Third, publications focusing on data security aspects in smart cities were studied. Semi-structured guided expert interviews with municipalities, technologists, researchers, private companies, and data security experts were conducted to describe the current situation in Germany.

Main findings show the need for an integrated security framework including threat and risk analysis. An important aspect is the requirement for a coherent data model. Data should be classified regarding to privacy demands and automated process integration (e.g. traffic control systems). Also, technical measures such as basic security for IoT-devices, end-to-end encryption, access control, digital signing, and a zero-trust network should be implemented. Institutions like the ENISA (European Network and Information Security Agency) or the German BSI (Federal Office for Information Security) will (have to) play a critical role in setting interdisciplinary standards and guidelines affecting the digitalisation of cities and therefore affecting the life of every citizen.

MÜHLBERG, JAN TOBIAS

Secure execution environments for critical sensing and control networks

dr. Jan Tobias Mühlberg, Imec-DistriNet, KU Leuven, Belgium

Abstract

Advanced societies increasingly rely on the security and reliability of critical infrastructure in domains such as the power grid, communication, transportation and medical infrastructure. Yet, sensing and control networks in these domains are subject to a growing number of attacks that put the safety of critical applications at risk. In the automotive domain, this already resulted in millions of vehicles being recalled. In other fields such as the power grid, public transportation or in medical networks, the consequences of such attacks can be life-threatening to large populations. However, even three years after the cyberwar over the Ukrainian power grid, most of our societies' critical infrastructure is unprotected and we do not understand threats and attackers very well.

The ICT security community has traditionally assessed the trustworthiness of applications at the software level, by reasoning about algorithms and source code as if it were executed on an idealised abstract computing platform. However, a recent line of hardware-level attacks -- Rowhammer, Meltdown, Spectre, and Foreshadow being prominent examples – revealed fundamental flaws in commodity hardware. There are two key lesson to be learned from this wave of microarchitectural vulnerabilities and the tiresome patching process: First, current processors exceed our levels of understanding and need to be subjected to independent review and assessment. Second, the development and validation of software for critical infrastructure must rely on a sound and highly detailed understanding of the execution environment -- cloud environments, processors, microcontrollers, and more. Without this, legal requirements such as the GDPR are hard to satisfy and the population at large may be subject to risks ranging from privacy breaches to physical harm at the hands of criminals.

In the context of smart cities, achieving the required level of understanding is particularly difficult: The execution infrastructure for software is inherently heterogeneous, widespread connectivity and a multitude of system interactions exist and can potentially be abused by attackers, and almost all system components must be considered critical or interact with critical equipment. Established attack schemes from the domains of automotive systems and smart grid infrastructure suggest that very strong attackers with code execution abilities on critical control units must be considered.

In this talk I will discuss how hardware-level vulnerabilities can hamper the security of even the most well-designed and well-implemented software systems. An ongoing line of research from imec-DistriNet at KU Leuven (BE) promises cross-platform mitigations and strong security guarantees for distributed control networks. I will elaborate on our experience with developing and integrating this technology in realistic control systems, e.g., in the automotive domain. Our work is based on Trusted Computing and heavily relies on security primitives in hardware, formal verification and hardware/software co-design. Over the

past five years we have published a number of processor designs, tools and prototypes, that exemplify the development of highly secure control systems for resource-constrained critical domains. The results of our work are freely available under open-source licenses.

PIANINI, DANILO

Computing at the aggregate level

dr. Danilo Pianini, University of Bologna, Italy

Abstract

In the vision of smart cities, pervasively deployed devices and humans will form ecosystems and collaborate to provide a wide range of services with the ultimate goal of improving our quality of life. To turn this vision into reality, however, a number of challenges need to be dealt with; arguably, these include handling dynamicity, heterogeneity, openness, and massive scale as well as embracing the "collective" dimension of systems. Aggregate Computing is an emerging paradigm for programming ensembles through a functional composition of "collective" behaviours, enabling scalability with system complexity, platform-independent system specification, inherent self-adaptation, and rigorous analysis of behavioural properties. We argue that Aggregate Computing can be beneficial to smart cities application development, and accordingly describe a number of key features and research directions.

Computer science

RUTLEDGE, LLOYD & BOS, JEROEN

A user interface template for semantic web-implemented Hohfeldian right and duty legal rules using the Fresnel data interface language

Prof. Lloyd Rutledge, OU Netherlands
(Jeroen Bos, OU Netherlands)

Abstract

This research applies Hohfeldian Right and Duty legal concepts to deliver an ontology-defined human-computer interface template. This approach facilitates adherence of end-user systems to the laws they help execute and must adhere to, and to the maintenance of these systems. Using the template, a user interface for Semantic Web-implemented legal rules can be delivered to support legal rule-driven applications. The template consists of a user interface specification ontology that refers to a target ontology.

This work presents the Legal Right and Duty Pattern (LRDP) as a Semantic Web ontology for Hohfeldian Right and Duty concepts. LRDP extends existing Hohfeld and user interfaces ontologies developed at the Open University of the Netherlands (OU) and elsewhere. We also present the more broadly applicable System User and Form (SUF) ontology. SUF is an extension of Fresnel, an established ontology for defining interfaces that browse Semantic Web-defined information. SUF's contribution to Fresnel is adaptation of system behavior to the current user and his current task. Combining SUF with LRDP defines how an information system adapts the information it presents and the features it provides to the current user according to his or her legal rights and duties in the context of the current activity.

For evaluation purposes, logic rules extracted from an actual law are mapped to the LRDP, SUF and Fresnel. The law used defines the Dutch Certificate of Good Behavior (Verklaring Omtrent Gedrag, or VOG). As such, this work builds upon related work implementing the VOG with Semantic Web-defined Hohfeld concepts by enriching Right and Duty support and adapting to the user and activity context. A partially functional mock-up is provided for a visual impression of a possible user interface implementation. The mock-up is implemented on the platform Semantic MediaWiki with the Page Forms extension, using existing tools that implement Fresnel on this platform. Our implementation on the Semantic Web enables use of Fresnel, provides well-supported logical reasoning and allows our technical results to apply to data on and from the Semantic Web, as well as more efficient development of systems from ontologies defined on the Semantic Web.

Law

BOOGAARD, HENK

The future of banks in times of artificial intelligence

Henk Boogaard, OU Netherlands

Abstract

What does the financial sector look like in the future? The financial sector is subject to major changes, with information technology playing a leading. Bankers will be replaced by IT professionals and banks will have to look for a new business model. The existing financial model is being attacked from all sides by front-runners in the field of artificial intelligence, working in combination with big data. The number of jobs and the macroeconomic importance of the sector is rapidly decreasing. On top of that, the image of the banking sector is struggling to recover since the 2008 global financial crisis.

In politics, the call for state intervention increases. Google, Apple and Amazon are the leaders in the field of artificial intelligence and are becoming increasingly active in the financial sector, with which the current financial institutions are unable to cope. In addition, banks lose market share to large international asset managers that have robot consultants working at low cost, and are facing competition from innovative fintech companies. The bank of the future will mainly operate via the internet, and social media will proactively inform and assist the customer with financial matters, especially via digital platforms. Smart apps will function as neutral intermediaries. These online platforms will collect the particular financial services and products that a consumer has with their financial service providers, and can then offer the possibility of requesting price offers from various suppliers from that platform. The customer has the upper hand. The European PSD2 directive gives the customer the right to demand that the information accumulated by the bank can be shared with others.

There is also concern for the banks on the corporate side. Peer-to-peer lending and crowdfunding are alternative forms of financing that can replace financing through banks. Recent financial initiatives make a good estimate of the creditworthiness of companies based on big data analysis of publicly available information. Therefore the focus will have to be on personal services, using the latest digital technologies. Banks will have to accelerate digitization and collaborate with innovative fintech companies. But there are also customers who are annoyed by digital applications and dealing with robots - they need and prefer personal contact with human experts. At the local level, there is a need, especially among the elderly, to be able to walk in somewhere.

What the future of the financial sector will look like tomorrow is still far from self-evident. Banks can embrace innovation and organize themselves more efficiently and effectively, have competitive advantages such as the possession of a banking license, and maintain the possibility to finance relatively cheaply through implicit support ('too big to fail' and the deposit guarantee system). The strict supervisory requirements offer them protection, too. The General Data Protection Regulation (GDPR) standardizes data protection legislation in all 28 EU countries and imposes strict new rules for the control and processing of personally identifiable information. As a result of the requirements that regulators impose, the compliance costs for new entrants are often prohibitive. But banks will not give up quickly.

Law

KARSTEN, JOOST

How law can create value for smart cities

Joost Karsten, OU Netherlands

Abstract

The concept of the "smart" city is a next step in controlling the current growth of cities. The evolution of society, as shown in this change of the structure of cities, comes with a wide variety of unknown challenges to control. The growth of the biggest cities, at the expense of smaller cities, results in a small amount of city proper. These metropoles have a hard time managing the ever expanding boundaries, among others because such growth comes with a rise in illegal and hidden activities.

The city council of a metropole can use data and artificial intelligence to improve control over these future challenges. In the case of artificial intelligence involvement a system based on logic is necessary. In order for a city to provide enough value for its inhabitants, the generation of value, the set of rules to control the value, and the execution of value by intelligent systems should all relate to the same concepts. A metropole will have to balance the interests of its citizens, visitors, and the businesses located in its proper, since they all relate to public interest. The growth of a city makes the conflicts of interest it will face more evident. And law has to keep up. Most future conflicts of interest can hardly be resolved using the current state of law. In case of the continuing rise of smart cities, law does not suffice. The upcoming conflicts of interest for future policy makers to deal with are based on concepts that should be understandable for human and artificial intelligence. These concepts should be based on information as a root of all further development and create an logic system for all disciplines to use. This system should follow the process from any given real world state to the value it can create. A city can create value if it can incorporate information networks with the highest gain in welfare and the lowest costs. The nodes in such information networks should collaborate in communicating information, maintaining the quality of information, interpreting the information, and take actions which generate the highest value. The maximum value any set of information networks can create might not equal all individual node value maximization options. Liability for any damage resulting from the use of information networks cannot be solved using our current legal system. Nor is the ownership of information owing through these information networks self-evident. Therefore generating public value has to be controlled by legislators and policymakers. Based on some general examples of conflicting interest I will showcase the value of using a logical system to deal with these challenges.

This system, based on mathematical concepts from information theory, game theory, and statistical distribution, follows the path any real world state takes to create value. The system uses information grids in order for cities to maximize value in different information networks. It also provides legislators and policymakers with a framework to incorporate artificial intelligence into the equation. Since it uses axiomatic and logical reasoning in the legal approach toward smart cities and the issue of conflicting interests. The framework makes it possible for legislators to provide sufficient rules and regulations to handle not only conflicting interest, but also interdependencies between the public, citizens, businesses, and visitors.

Law

RINKES, JAC

Smart cities: Citizenship for robots and legal aspects of autonomous driving

Prof. dr. Jac Rinkes, OU Netherlands

Abstract

The present conference theme is 'the smart city': urban development in the sustainability transition promises efficient reorganization of the flows of resource, goods, services and people, drawing on sensor technologies and artificial intelligence. This development requires a fundamental rethinking of the way the law contributes to society. Two focal points are the emergence of AI, artificial intelligence (robots vs man), and the legal aspects of new technologies and safety issues. The first issue regards the concept of citizenship and the question whether a legal niche is available for AI in the present and future society, giving robots full rights of citizenship. The second issue focuses presently on the emergence of autonomous driving and its legal implications. In this paper, these issues will be addressed from a rule of law/legal point of view.

Citizenship and AI

AI is a reality: algorithms are already a substantial part of society, and have presented a latitude of legal questions. The question is whether algorithms and the machines they instruct should be seen as useful automated helpmates for humans, or whether they could be seen as autonomous beings (persons with human or similar rights). Will we continue to use computers ourselves, or will computers structure society and our environment and leave us to do other things (more useful?). The 2018 case of Yoshitaka Sakurada, deputy chief of Japan's cybersecurity strategy office could be exemplary: Sakurada has never used a computer and seemed confused by the concept of a USB drive when asked. He replied: since the age of 25, I have instructed my employees and secretaries, so I don't use computers myself. That is obviously the best cybersecurity, but seen from a different point of view: in the advent of AI, why should humans need to continue to use computers and (try to) be masters of machines much more advanced than men? And if man abandons the idea to keep up with the development of AI, how will computers react? (compare the well-known thought experiment how AI would free itself from humans, by imagining that you find yourself as a superintelligent human on a planet inhabited only by 5 year-olds. What would you do in order to become an autonomous master of the planet?). Fears of this nature have fueled the desire to develop specific legal rules for AI, starting with Asimov's three rules for robots. (homo sapiens sapiens – now alone in the human world - has never tolerated other sorts of humans in its vicinity, otherwise we would still have the benefit of the existence of multiple and varied types of humans). A perspective that could be helpful in developing these rules could be passed on the concept of citizenship. It has taken man a long time to develop basic rules for society (war and terror reigned for thousands of years). The recognition (and discovery) of the rule of law seems presently the only viable basis for peaceful and sustainable societies, respecting safety and security, and avoiding the destruction of our environment and living conditions. The issue is not what rights AI/robots should acquire, but how they should be able to function in human society. What are the duties that are a necessity for a peaceful functioning of man and robot in society? These are mainly of a moral and ethical nature, and focus on behavior. Basically, these rules are not laid down in laws and regulations: they are of a different nature (Durkheim). First, citizens (and I include AI if these machines should become members of society and not just helpful machines) have obligations towards the state and community: we should always obey law and our government, within the borders of the rule of law, fundamental rights and freedoms. This provides order and system (and should therefore be attractive to human-like AI). Secondly, humans and robots alike should be just, fair, honest, charitable and loving towards each other, thus preventing disorder and disturbance. A third duty is the promotion of science, knowledge and culture. Unity and tolerance are further duties: discord and disharmony lead to suspicion and mistrust, and are detrimental to prosperity. Citizens (human and AI) should accept responsibility for their conduct and acts, and contribute fully to society and its goals. Within these boundaries, further legal rules

regarding the functioning of AI in society should be developed. In this paper the implications of this road map for legislators will be developed.

Autonomous driving: a legal perspective

It is commonly accepted that cars without drivers still need a moral compass. This requires an assessment of ethical dilemmas, and tough choices (Edmonds 2018: would you kill the fat man?). A favorite starting point is the so-called trolley problem (a runaway train and choices to be made when changing a signal). Midgely thought the trolley problem to be a depressing example of academic philosophers' obsession with concentrating on selected, artificial examples so as to dodge the stress of looking at real issues. The engineering challenges are tough, but the ethical challenges may be even more difficult to overcome. In general, driverless cars will be very beneficial to society (less isolation for fearsome drivers, no time wasted behind the wheel, better environment, life-saving – no more driver errors or stupidities such as drink-driving or using mobile phones while driving). So in general: driverless cars will benefit society (although professional drivers will have to look elsewhere for employment). Only in rare and unusual cases morals should be programmed into the car. What is the best solution: maximize happiness for all, save as many lives as possible, humans are not objects to be used at will. Edmonds expects that ultimately utilitarian solutions should prevail: then, it will make no longer sense to hold humans culpable for machine actions, especially if machines are self-learning and might behave in unforeseen ways. Safety rules are limited in effectiveness and enforcement (a good example can be found in the New Zealand Bunnings sausage safety rules). Minimize loss of lives and maximize safety for citizens seem to be the mantras of autonomous driving. This paper examines the viability of this perspective when laying down legal rules for driverless cars.