Intelligent Campus: Risks, Benefits and Ethics

Andrew Cormack[1]

[1] Jisc, Lumen House, Library Avenue, Didcot, OX11 0SG, UK, Andrew.Cormack@jisc.ac.uk

…

Keywords
Intelligent Campus, Smart City, Data Protection, Ethics.

SUMMARY

The Intelligent Campus is a microcosm of the Smart City. Smart cities, according to Finch and Tene (2016), may be 'more livable, more efficient, more sustainable and more democratic' or 'turn into electronic panopticons in which everybody is constantly watched'. Intelligent Campuses amplify both of these possibilities since – unlike cities where space and data are owned by many different organisations – a university may well control and monitor the whole physical and digital infrastructure of its students' lives, from bed to workplace to social spaces. Students and staff might well consider such monitoring 'creepy', or worse. But that single control, and the strong shared interest between campus managers and occupants, may make the goal of smart citizenship easier to achieve on campus than in cities, where political and commercial interests have largely limited the relationship to a paternalistic one, at best. This talk will present practical tools to help educational institutions deliver this goal.

EXTENDED ABSTRACT

Our responses to monitoring depend not only on fact, but on sentiment. Attitudes to electronic monitoring, in particular, are often set by the behaviour of social networks and other commercial service providers. Campus occupants used to hearing that they are 'the new oil' (Kuneva, 2009) or 'digital silkworms' (Brown & Marsden, 2013) need to be reassured about the purposes, intentions and incentives of those who monitor, as well as how monitoring is currently performed. Campus managers therefore need to ensure their plans and actions are acceptable to both their organisation and the campus occupants. If not, occupants may well respond by changing behaviour – for example swapping identities or providing deliberately incorrect data – in ways that undermine both the intelligent campus and, more importantly, the institution's primary purposes of research and education.

As well as smart city literature, tools borrowed from other fields can guide us towards intelligent campuses that are welcomed by their occupants. Many issues are shared with Radio Frequency Identification (RFID) technologies, for which a toolkit was endorsed by European Data Protection Regulators in 2011. When selecting appropriate purposes for intelligent campus technologies, ethics codes on using digital data for research and policy formation are also relevant.

Intelligent campuses can be viewed as having three 'senses': sight, sound and location. Sight includes Passive Infra-Red (PIR) sensors that indicate whether or not a desk is occupied, and face recognition analysis of live video images; sound can record conversations, or detect whether a room is empty; location and movement of devices and individuals can be gathered from wireless access points, door access or payment cards. As these examples indicate, all three senses cover a similar, wide, range of intrusiveness. Rather than ranking the senses, it is better to generalise and extend the four-level scale of impact from RFID guidance: presence, counting, identifying, recording and analysing. This gives an immediate indication of the likely level of intrusiveness, and the depth of analysis and mitigation likely to be required.

The context from which information is gathered can significantly affect both intrusiveness and perception. A standalone PIR desk-occupancy monitor is much less intrusive in a hotdesk area than in a personal, locked office, or if its data are linked to login or other information that can identify individuals. Some spaces, such as bedrooms, offices and toilets, are obviously more sensitive, but universities may also have spaces such as counselling services and some laboratories where monitoring,

and its results, require particular protection. Sight sensors naturally respect opaque boundaries, such as walls, but sound and location may leak through them.

While an extended version of the RFID toolkit provides guidance on controls – such as organisation and policy, system architecture, sensor choice, and other risk reduction measures familiar when protecting personal data – these may be insufficient to ensure acceptability. For this we need to consider not just legal questions ('what **can** we do?') but also ethical ones ('what **should** we do?'). Kitchin (2016) identifies six ethical concerns for smart cities: datafication, dataveillance and geosurveillance; inferencing and predictive privacy harms; anonymisation and re-identification; obfuscation and reduced control; notice & consent empty or absent; data use, sharing and repurposing. The Menlo Principles (Homeland Security, 2012) for digital research ethics and the UK Government's Data Science Ethical Framework (Cabinet Office, 2016) for policy formation reinforce the need for organisational controls, but add choice of purpose; robust models (in both theoretical and data science senses); and awareness of – possibly changing - public perception.

One of the greatest challenges in both smart cities and intelligent campuses is to ensure that occupants are informed about data collection and use. Much data collection takes place through passive observance, unconnected to any specific action by the individual (entry and payment cards are a rare exception); many 'internet of things' sensors are designed to be unobtrusive. Individual occupants may well be, or become, unaware of data collection, reducing the effectiveness of traditional protections such as notice, consent and objection. In any case, it is often unreasonable to rely on individual actions to control risk: individuals cannot realistically avoid using campus infrastructures, and should not be burdened with daily, or even more disruptive, consent decisions.

The concept of 'smart citizenship' may well help with this transparency challenge, as well as identifying acceptable uses of intelligent campus technologies and holding institutions accountable for their activities. Rather than viewing citizens as 'consumers or testers', authors such as Cardullo and Kitchin (2018) propose involving them from the start in the selection, design and monitoring of smart city (or intelligent campus) projects. Policies or proposals that feel unfair, creepy, or worse, to citizens will then be discovered – and improved or rejected – at an early stage, before money or infrastructure has been deployed. Such an approach also reflects the ethical need to be aware of public sentiment, and the legal requirement for Data Protection Impact Assessments to consider consultation with individuals. Smart citizens guide the development of their city, rather than merely occupying it. The complexity of cities has, so far, prevented the achievement of this concept. The simpler organisational structure of an intelligent campus might be an opportunity to show how it can be done.

References

Brown, I & Marsden, C. (2013) *Regulating Code: Good Governance and Better Regulation in the Information Age*. Cambridge: MIT Press.

Cabinet Office. (2016) *Data Science Ethical Framework (Version 1.0)*. Retrieved January 29, 2019, from https://www.gov.uk/government/publications/data-science-ethical-framework

Cardullo, P & Rob Kitchin, R. (2018) Being a "citizen" in the smart city: up and down the scaffold of smart citizen participation in Dublin, Ireland. *Geojournal*, 10.

Finch, K & Tene, O. (2016) Welcome to the Metropticon: Protecting Privacy in a Hyperconnected Town. *Fordham Urban Law Journal*, 41(5), 1581-1615.

Kitchin, R. (2016) The ethics of smart cities and urban science. *Philosophical Transactions of the Royal Society A*, 374.

Kuneva, M. (2009) *Keynote Speech: Roundtable on Online Data Collection, Targeting and Profiling*. Retrieved January 29, 2019, from http://europa.eu/rapid/press-release_SPEECH-09-156_en.htm

Homeland Security. (2012) *The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research*. Retrieved January 29, 2019, from https://www.dhs.gov/sites/default/files/publications/CSD-MenloPrinciplesCORE-20120803_1.pdf

Andrew Cormack is Chief Regulatory Adviser at Jisc, responsible for informing the company and its customer universities, colleges and schools about the regulatory implications of services based on networks and data. He responds to UK and EU consultations and enquiries in these areas. He is an experienced speaker, having given invited keynotes at TERENA (2011) and EUNIS (2018) conferences and led an EU Presidency Ethics & AI workshop (2019), as well as many presentations at national and international conferences. He was Programme Committee Chair for the TERENA conference in 2009, and the FIRST Computer Security and Incident Response Conference in 2019. He has written more than 500 blog posts on legal and technical issues.

Previously he was Head of CERT for Janet, running the incident response team for the UK's National Research and Education Network (1999-2002); Systems Programmer at Cardiff University, responsible for the development, management and security of web, news and email services (1994-1999) and Senior Scientific Officer at NERC's Research Vessel Services, responsible for developing scientific computer systems and providing onboard support during oceanographic research cruises (1989-1994).

Andrew was Chair of the Funding Council of the Internet Watch Foundation from 2009-2013, a member of the Permanent Stakeholders Group of ENISA from 2004-2014, and of the Board of ORCID from 2017-2019. In 2015 he was awarded the Vietsch Foundation Medal for his role in advancing trust and security within the European research and education sector.

Andrew has an MA in Mathematics from Cambridge University (1988), LLB (2006) and BA(Humanities) (2010) from the Open University, and a Masters in Computer and Communications Law (2015) from Queen Mary, University of London. His LLM dissertations – "Is the Subject Access Right now Too Great a Threat to Privacy?" and "Do Generic gTLDs Need Their Own Ex Ante Regulation?" – were both published in 2016, and he has continued to publish in academic journals in the areas of Incident Response and Data Protection, Learning Analytics, Big Data, and the Intelligent Campus.

He enjoys hill-walking, birdwatching and cooking.