See No…, Hear No…, Track No…: Ethics and the Intelligent Campus

Andrew Nicholas Cormack*

Intelligent Campus Possibilities

Jisc subtitles its Intelligent Campus guide 'Using Data to Make Smarter Use of Your University or College Estate'.[1] Combining data from sensors around campus, and from the people and things that are present on it, could help with 'improving the student experience… creating new opportunities for research… reducing environmental impact… enhancing the physical environment… maximising use of valuable resources'.[2] However there are also risks: most obviously that students, staff and visitors will feel they are being tracked, checked or surveilled;[3] but also of misinterpretation, both by campus occupants as to what monitoring is for,[4] and by campus managers as to its purpose and meaning.[5] Jisc concludes '[t]here is a responsibility on those designing and implementing applications within the intelligent campus to provide reassurance and effective management'.[6]

Many of these concerns have been discussed in the context of Smart Cities – not surprising as

> The campus is in many ways a city in microcosm. Lancaster University comprises over 288 buildings, which include offices, lecture halls, laboratories, small business incubators, a theater, a library, a sports center, shops, and residences. There are 13,300 students, of which over 7,000 live on campus during term time. There are 2,350 employees and numerous visitors and service delivery personnel.[7]

Kitchin notes different perspectives on the smart city: it may be a data-centric 'everyware'; offer improved policy, development and governance; be citizen-centric, with real engagement in decision-making; or all three.[8] According to Finch and Tene, smart cities may be 'more livable, more efficient, more sustainable and more democratic' or 'turn into electronic panopticons in which everybody is constantly watched'.[9] Galdon-Clavell points out the small difference in perception, and none in technology, between these outcomes: 'understanding smart technologies as surveillance-enabled technologies ... puts the debate in a different place'.[10]

---

* Chief Regulatory Advisor, Jisc Technologies

[1] Jisc, 'The Intelligent Campus: Using Data to Make Smarter Use of Your College or Campus Estate' (2018) < https://repository.jisc.ac.uk/6882/1/Intelligent_Campus_Guide.pdf > accessed 14 February 2019.

[2] Jisc, 'The Intelligent Campus' *supra* n 1, 12.

[3] Jisc, 'The Intelligent Campus' *supra* n 1, 26.

[4] Jisc, 'The Intelligent Campus' *supra* n 1, 24.

[5] Jisc, 'The Intelligent Campus' *supra* n 1, 24.

[6] Jisc, 'The Intelligent Campus' *supra* n 1, 25.

[7] Oliver Bates and Adrian Friday, 'Beyond Data in the Smart City: Repurposing Existing Campus IoT' [2017, April-June] IEEE Pervasive Computing 54, 55.

[8] Rob Kitchin, 'The Promise and Perils of Smart Cities' [2015, June/July] Computers and Law < https://www.scl.org/articles/3385-the-promise-and-perils-of-smart-cities > accessed 14 February 2019.

[9] Kelsey Finch and Omer Tene, 'Welcome to the Metropticon: Protecting Privacy in a Hyperconnected Town' (2016) 41(5) 1581, 1583.

[10] Gemma Galdon-Clavell, '(Not so) smart cities?: The drivers, impact and risks of surveillance-enabled smart environments' (2013) 40 Science and Public Policy 717, 720.

A benevolent smart city – or campus – is therefore not just about how its sensors and data are used, but how they are perceived. According to Edwards, 'public trust and confidence in technologies are generally regarded as vital to their uptake', but there is a 'crisis of confidence about privacy and trust in IoT environments'.[11] One of the main features of internet-connected 'things' – that they are 'explicitly designed to be as unobtrusive and seamless as a user experience' – contributes to this.[12] With privacy discussions often dominated by 'Notice and Consent',[13] a device that is designed not to be noticed is bound to have an inherent trust problem.

Several authors seek a solution in individual choice. For example Bernal: 'To be autonomous, therefore, meaningful choices have to be present and one needs to be given the opportunity to make those choices, appropriately informed and free from coercion, restraint, or excessive or undue influence'.[14] But when public – and some private – spaces are continually monitored, free choice may be impossible: citizens have 'no ability to opt out other than to avoid the area, which is unreasonable and unrealistic' (Kitchin);[15] 'data disclosures by residents in a "smart city" simply cannot be avoided' (Edwards).[16] In such situations consent may become 'an empty exercise'[17] to 'rubberstamp patterns of data collection which are increasingly damaging for society'.[18] Normal data protection safeguards may have limited force: as Kitchin observes 'if a person is unaware that data about them are being generated, then it is all but impossible to discover and query the purposes to which those data are being put',[19] while organisations that protect privacy by not collecting identifying data may be unable to verify the identities of those who claim to exercise individual rights.[20,21]

These issues apply equally to the intelligent campus: indeed its geography, infrastructure and governance may increase the risks. However they may also provide more opportunities to address the challenges.

In a smart city, individuals are most likely to be monitored as they move around, in public spaces and public buildings. In workplaces they may be monitored by their employer, in shopping malls by individual shops, but there are commercial, legal and often technical barriers to sharing or correlating this raw data with city systems outside.[22] Within the home,

[11] Lilian Edwards, 'Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective' (2016) 2(1) European Data Protection Law Review 28, 41.
[12] Edwards, 'Privacy, Security and Data Protection in Smart Cities' *supra* n 11, 42.
[13] Rob Kitchin, 'The ethics of smart cities and urban science' (2016) Philosophical Transactions of the Royal Society A 374, 9 < http://dx.doi.org/10.1098/rsta.2016.0115 > accessed 14 February 2019.
[14] Paul Bernal, *Internet Privacy Rights: Rights to Protect Autonomy* (1st edn, Cambridge University Press 2014), 25.
[15] Kitchin, 'The ethics of smart cities and urban science' *supra* n 13, 9.
[16] Edwards, 'Privacy, Security and Data Protection in Smart Cities' *supra* n 11, 39.
[17] Kitchin, 'The ethics of smart cities and urban science' *supra* n 13, 9.
[18] Edwards, 'Privacy, Security and Data Protection in Smart Cities' *supra* n 11, 55.
[19] Kitchin, 'The ethics of smart cities and urban science' *supra* n 13, 9.
[20] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 11.
[21] Andrew Cormack, 'Is the Subject Access Right Now Too Great a Threat to Privacy?' (2016) 2(1) European Data Protection Law Review 15, 18.
[22] Paolo Cardullo and Rob Kitchin, 'Being a "citizen" in the smart city: up and down the scaffold of smart citizen participation in Dublin, Ireland' (2018) Geojournal, 7 <https://doi.org/10.1007/s10708-018-9845-8> accessed 14 February 2019.

occupants can normally choose whether or not to install and maintain sensors.[23] By contrast, in an intelligent campus, the campus manager can install sensors in workplaces, public and social spaces, and – at least for many students – accommodation. The physical boundaries that delimit or separate monitoring regimes in the smart city are much less effective in an intelligent campus.

As Bates and Friday highlight,[24] the same campus infrastructure covers places where people work, sleep and play. Students (and, in some cases, staff) expect the same network connectivity in their bedrooms as their lecture theatres. Even more than in a smart city, a student or lecturer has 'few alternatives to [authority]-operated sensors and surveillance technologies increasingly deployed throughout their environs'.[25] In a smart city, it may still be possible for an occupant to choose different utility providers, walking routes, etc.[26,27] to make it harder to collect and combine sensor data about them: this is much more difficult harder on a smart campus.

Governance in a smart city is typically complex involving, according to Dameri and Benevolo, competing stakeholders with different goals.[28] In Genova, the Smart City Association has 'more than 40 members, including public bodies, research bodies, large companies, small- and medium-size enterprises, trade associations, and not-for-profit organisations'.[29] Tracing accountability may, according to Kitchin, involve a 'maze-like assemblage of data flows and controllers'.[30] Smart campuses, by contrast, typically have a single controlling organisation whose goals should, in principle, align with those of their staff and students to learn and research.

Simple governance represents both a threat and an opportunity. Individuals may well be concerned at a single entity having such detailed knowledge, especially given the university or college's importance for their current employment and future career prospects.[31] But simple governance also makes it easier for the controlling organisation to choose its preferred approach, in particular to implement the trust measures prescribed by Lane et al for smart cities:

> identif[y] the legal status of those bodies holding data; develop[] agreed and common standards covering data security and authentication of … users; develop[] public support for the use … of de-identified personal information; creat[e] a coordinated governance structure for all activities associate with access, linking and sharing personal information.[32]

An intelligent campus may therefore find it easier than a smart city to follow Galdon-Clavell and develop 'privacy-enhancing smart technologies and privacy-protecting regulatory

---

[23] E.g. Mara Ballestrini, Paul Marshall, Tomas Diez, 'Beyond Boundaries: the home as city infrastructure for smart citizens' (2014) UbiComp Adjunct, 988 <http://dx.doi.org/10.1145/2638728.2641557> accessed 14 February 2019.

[24] Bates and Friday, 'Beyond Data in the Smart City' *supra* n 7, 55.

[25] Finch and Tene, 'Welcome to the Metropticon' *supra* n 9, 1595.

[26] Cardullo and Kitchin, 'Being a "citizen" in the smart city' *supra* n 22, 7.

[27] Finch and Tene, 'Welcome to the Metropticon' *supra* n 9, 1595-6.

[28] Renata Paola Dameri and Clara Benevolo, 'Governing Smart Cities: An Empirical Analysis' (2016) 34(6) Social Science Computer Review 693, 695.

[29] Dameri and Benevolo 'Governing Smart Cities' *supra* n 28, 702.

[30] Kitchin, 'The ethics of smart cities and urban science' *supra* n 13, 9.

[31] Jisc, 'The Intelligent Campus' *supra* n 1, 28.

[32] Julia Lane, Victoria Stodden, Stefan Bender, Helen Nissenbaum, *Privacy, Big Data and the Public Good* (1st edn, Cambridge University Press 2014), 134.

frameworks'.[33] Edwards, noting that mere legal compliance may be insufficient to address the challenges of both practice and perception, suggests doing this through 'holistic privacy impact assessments (PIAs)';[34] prohibiting some activities, even if formally 'consented', as 'toxic';[35] and providing tools to help individuals understand what is being done with their data.[36]

This paper therefore proposes a mechanism for conducting privacy impact assessments in an intelligent campus, extending and generalising a framework approved by European regulators for Radio-Frequency Identification (RFID) systems; considers specific intelligent campus issues when attempting to mitigate privacy impacts; uses ethical codes to help identify the applications that campuses should be implementing; and applies smart city literature to propose new roles for both campus managers and occupants. In an intelligent campus, as Kitchin concludes for smart cities 'managers need to … take a pro-active role in brokering privacy and security arrangements on behalf of citizens';[37] campus occupants should no longer be considered just as individuals responding to the infrastructures they inhabit, but given the power to collectively participate in the choice, design and review of the systems they want to make their campus better.

Intelligent Campus Senses

An intelligent campus can typically detect humans using three 'senses': video, audio and location. Common examples of video are CCTV and motion sensors; audio is less common, but microphones are used to monitor noise levels and may be included in some CCTV systems; location often involves mobile devices – either by external observation of their Bluetooth, WiFi or mobile phone transmissions or by devices determining their own location using sensors such as GPS – but also fingerprint readers, swipe and payment cards that are presented at particular, known, locations such as doors or shops.[38]

While it is tempting to rank these senses by intrusiveness, all three can in fact be used in both intrusive and non-intrusive ways. Vision can be used to sense whether a room is full or empty, or to track individuals using face recognition; hearing can be used to measure activity in a space, or to record conversations and recognise individuals; location can provide approximate headcounts, or track an individual and their contacts throughout the day and night.[39] Although laws, such as the *Investigatory Powers Act 2016*, have traditionally distinguished 'metadata' (including location) from 'content' (video and audio), and awarded lower protection to the former, many authors have argued that both are now equally intrusive. Bernal considers 'the separation into the two categories is based to a great degree on an old-fashioned view of communications';[40] in *Tele2/Watson* the European Court of Justice found that communications metadata 'is no less sensitive, having regard to the right to privacy, than

[33] Galdon-Clavell, '(Not so) smart cities?' *supra* n 10, 718.
[34] Edwards, 'Privacy, Security and Data Protection in Smart Cities' *supra* n 11, 29.
[35] Edwards, 'Privacy, Security and Data Protection in Smart Cities' *supra* n 11, 56.
[36] Edwards, 'Privacy, Security and Data Protection in Smart Cities' *supra* n 11, 29.
[37] Kitchin, 'The ethics of smart cities and urban science' *supra* n 13, 12.
[38] Lorna Woods, 'Automated Number Plate Recognition: Data Retention and the Protection of Privacy in Public Places' (2017) 2(1) JIRPP, 10 <http://doi.org/10.21039/irpandp.v2i1.35> accessed 14 February 2019.
[39] Irina Raicu, 'Students and Sensors: Data, education, privacy, and research' (Markkula Centre for Applied Ethics, 31 July 2018) <https://www.scu.edu/ethics/focus-areas/internet-ethics/resources/students-and-sensors-data-education-privacy-and-research/> accessed 14 February 2019.
[40] Bernal, *Internet Privacy Rights: Rights to Protect Autonomy supra* n 14, 106.

the actual content of communications'.[41] Likewise in *Big Brother Watch*, the Court of Human Rights was 'not persuaded that the acquisition of related communications data is necessarily less intrusive than the acquisition of content'.[42] The intrusions caused by the three senses are different, but their impact on privacy and other fundamental rights can be equally serious. To assess the risk from a particular intelligent campus application, the characteristics of the application are more relevant than the particular sense it currently uses.

Application characteristics, rather than specific technologies, are the focus of a framework for Radio Frequency Identification (RFID) systems that was endorsed by the Article 29 Working Party in its Opinion 9/2011.[43] This categorises applications using a four-point scale:

- Level 0: RFID tags unlikely to be carried by an individual
- Level 1: RFID tags likely to be carried by an individual, but the application does not process or link to personal data
- Level 2: Application processes/links to personal data, but RFID tag does not contain it
- Level 3: Application processes/links to personal data, and tag contains personal data[44]

Since RFID tags are a location sense already deployed on campuses (for example in access cards and library books[45]), this framework might be applicable to the Intelligent Campus. As discussed below, law, cases and commentary on location and vision senses suggest that Levels 0, 1 and 2 can indeed be mapped directly to this wider context; Level 3 requires a generalisation of the 'storage' concept; and a new Level 4 is required at the top of the scale. Thus Intelligent Campus applications can be classed on a five point scale:

- Presence (Level 0): whether a space is occupied, including whether there are a small or large number of occupants. This could include, for example, sensing the level of noise, the number of wireless connection requests, or motion detection. No processing of identifiable information is needed, even to derive the occupancy.
- Counting (Level 1): referred to as 'statistical counting' in the draft ePrivacy Regulation.[46] The canonical example is measuring queuing time by calculating how long wireless devices are stationary before moving past a bottleneck. This does require monitoring the location of individual devices over a short period, but for this calculation there is no need to link their identifiers to their users, to any other information source, or to the desired output.
- Identifying (Level 2): including, as discussed below, 'singling out' in the Article 29 Working Party guidance.[47] These applications do associate sense information with individuals, either to link to other information sources such as their name or subject,

[41] Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson, Peter Brice, Geoffrey Lewis* [2016] ECLI:EU:C:2016:970 para 99.
[42] *Big Brother Watch and others v UK*, nos. 58170/13, 62322/14 and 24960/15, ECHR 2016 para 356.
[43] Article 29 Working Party, 'Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications' (2011) 00327/11/EN WP 180.
[44] Article 29 Working Party, 'Privacy and Data Protection Impact Assessment Framework for RFID Applications' (12 January 2011) WP 180 Annex, 7.
[45] Ken Young, 'Shelf Life' (Guardian, 11 Nov 2004) <https://www.theguardian.com/technology/2004/nov/11/onlinesupplement.insideit> accessed 14 February 2019.
[46] Council of the European Union, 'Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - Examination of the Presidency text' (Council of the European Union, 5 December 2017) 15333/17, Recital 25.
[47] Article 29 Working Party, 'Opinion 4/2007 on the Concept of Personal Data' (2007) 01248/07/EN WP 136, 17

or to provide personalised services. Monitored CCTV and mobile apps that are aware of their current location will generally fall into this category.

- Recording (Level 3): systems that record sense data for occasional later processing, for example recording of CCTV or door entries in case they are subsequently needed to investigate an incident.
- Analysing (Level 4): systems that involve automated analysis of sense data, such as face recognition, audio analysis for trigger words, or mapping of behaviour or relationships between individuals.

For applications using Presence, Level 0, no data relating to identified, or identifiable, individuals[48] is required, even ephemerally. Counting is done either using physics – e.g. level of sound or movement – or directly in hardware – e.g. number of radio broadcasts seen. Where presence information is calculated by counting the number of distinct identifiers broadcasting, this should be treated as a Level 1 application.

Although the Working Party seems to have doubted in 2011 whether Level 1 applications would exist – 'in most scenarios, if the tag is destined to be carried by a person it would qualify as a level 2 application and not a level 1 application as suggested by the Framework'[49] – subsequent developments in both the *General Data Protection Regulation* (GDPR) and draft *ePrivacy Regulation* have confirmed this category. According to the European Court of Justice in *Breyer*, identifiers (such as MAC or IP addresses) associated with devices that have authenticated to the campus network must be considered personal data since the network operator will have lawful and practical means, even if it does not use them, to associate the identifier with the authenticated user.[50] The Article 29 Working Party's comments on identifiers that let an individual be 'singled out' suggest that even identifiers from devices that have not authenticated should also be treated as personal data.[51] Applications that process these identifiers cannot, therefore be Level 0. However Recital 28 and Article 4(5) of the GDPR encourage organisations to reduce the risk of processing by treating such identifiers as pseudonyms, keeping the information needed to link to the individual separate, if they have it at all.[52] When considering the use of signals emitted by mobile devices, the European Commission's proposal for an *ePrivacy Regulation* distinguishes a group of applications 'including people counting, providing data on the number of people waiting in line, ascertaining the number of people in a specific area, etc.' from 'more intrusive purposes, such as to send commercial messages to end-users for example when they enter stores, with personalized offers'.[53] The Council of Ministers notes that the former can be done using pseudonyms and additional protections:

> such counting [must be] limited in time and space to the extent necessary for this purpose. Providers should also apply appropriate technical and organisations measures to ensure the level [of] security appropriate to the risks, including pseudonymisation of the data and making it anonymous or eras[ing] it as soon it is [no] longer needed for this purpose. Providers engaged in such practices should

[48] *General Data Protection Regulation supra* n 20, Article 4(1).
[49] Article 29 WP, 'Framework for RFID Applications' *supra* n 43, 5-6.
[50] Case C-582/14 *Breyer v Germany* [2016] ECLI:EU:C:2016:779 paras 46-48.
[51] Article 29 WP, "Personal Data" *supra* n 47, 17.
[52] *General Data Protection Regulation supra* n 20, Article 4(5).
[53] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) COM(2017) 10 final 2017/003 (COD), Recital 25.

> display prominent notices located on the edge of the area of coverage informing end-users prior to entering the defined area…[54]

Applications of this type, which the European Parliament calls 'mere statistical counting',[55] therefore fall into Level 1, Counting, distinguished from applications in higher categories that involve singling out an individual device or tracking it over an extended period.

The Article 29 Working Party's comments on RFID systems make clear that Level 1 applications are a limited exception. Most location-aware applications will fall into Level 2, Identifying, or above. This is most obvious when they link sense data to other information about the individual: for example their lecture timetable in the case of a navigation app that guides students to events at the right time; their study record in the case of an application that reminds them when they are passing the library; or their identity and authorisation to enter a part of a building in the case of a door-entry smartcard. Regulators have been clear that any action that singles out an individual for specific treatment (such as alerting them to offers from a favourite coffee shop) falls into the same risk category even if it does not involve identifying the individual by name, email address, etc.[56] Though live CCTV monitoring, without recording, of public places has been considered not to engage privacy rights in legal cases (for example *Rynes*[57] and *Catt*,[58] discussed below), the Surveillance Camera Commissioner considers that all deployments should be preceded by a data protection impact assessment.[59] This suggests that any video, audio or location data that is simultaneously monitored by humans should also be classed as Level 2 or higher. This applies particularly in the campus context, where some of the spaces monitored may be considered private or sensitive, as discussed below.

Level 3, Recording, has been distinguished from mere observation by courts in a number of cases. For example, Woods notes that in *Catt*, the UK Supreme Court judges 'were unanimous' that 'mere observation [of a public place] cannot, save perhaps in extreme circumstances engage Article 8, but the systemic retention of information may do'.[60] While *Catt* concerned photographs, in *Peck* the European Court of Human Rights confirmed that 'the recording of [CCTV] data and the systematic or permanent nature of the record may give rise to such considerations'.[61] In *PG and JH* the same court confirmed the significance of recording speech, even though the purpose was to obtain a voice sample, rather than the content of what was said.[62] Woods detects courts expressing concern about 'locational privacy' when individuals' locations are 'systematically monitored and/or recorded'.[63] In each case, the concern seems to be that a recording could be 'used for purposes other than to

[54] Examination of the Presidency text, *supra* n 46, Recital 25.
[55] European Parliament, 'Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Report' (European Parliament, 23 October 2017) A8-0324/2017, Amendment 27.
[56] Article 29 WP, "Personal Data" *supra* n 47, 17.
[57] Case C-212/13 *Ryneš v Úřad pro ochranu osobních údajů* [2014] ECLI:EU:C:2014:2428 paras 22-25.
[58] Woods, 'Automated Number Plate Recognition' *supra* n 38, 10.
[59] Surveillance Camera Commissioner, 'Data Protection Impact Assessments for Surveillance Cameras' (Surveillance Camera Commissioner, 2018), 2 <https://www.gov.uk/government/publications/data-protection-impact-assessments-for-surveillance-cameras> accessed 14 February 2019.
[60] Woods, 'Automated Number Plate Recognition' *supra* n 38, 10.
[61] *Peck v UK*, no. 44647/98, ECHR 2003, para 59.
[62] *PG and JH v UK*, no. 44787/98, ECHR 2001, para 59.
[63] Woods, 'Automated Number Plate Recognition' *supra* n 38, 10.

keep a watch on places'[64] or, in data protection terms, that there is a risk of breaching the purpose limitation principle. In particular, recordings can be reprocessed for purposes not envisaged at the time of collection, for example because an individual becomes newly of interest (Georgetown's Centre for Privacy and Technology note the possibility to 'investigate a person's past behavior'[65]) or because new technologies allow processing in ways that were impossible at the time of collection (Woods notes the possibility of 'retrospective vehicle tracking' using Automatic Number Plate Recognition (ANPR) records[66]). As the RFID Framework recognises, recordings also extend the time and scope over which a privacy risk exists or may be created: whether by intended or unintended access. For example a historic collection of New York taxi trip records revealed the identity of regular customers of a nightclub, even though there was no passenger information in the dataset.[67]

Although the law has not yet distinguished Level 4, Analysing, from Level 3, the UK's Information Commissioner (ICO) has described the addition of face recognition to CCTV as 'a real step change in the way law-abiding people are monitored as they go about their daily lives'.[68] Some of the problems highlighted by the ICO and Electronic Frontier Foundation[69] relate to the current state of the technology: error rates and discrimination risks may be reduced in future. However there are more persistent concerns about the continuous nature of the surveillance (as opposed to the episodic re-processing of sections of interest from a recording) and how to justify and protect the extensive processing of those who are not targets of interest. For example when face recognition was used in a shopping centre to identify missing persons and those wanted for crimes the UK's Surveillance Camera Commissioner noted that 'compared to the size and scale of the processing of all people passing a camera, the group they might hope to identify was miniscule'.[70,71] As well as these direct risks, people are likely to respond to this level of intrusiveness by changing behaviour: indeed the claimants in *Herbecq* suggested that the 'deterrent effect' of CCTV on lawful behaviour might be deliberate.[72] Edwards notes the wearing of hoodies as a response to

[64] *Pierre Herbecq and the Association Ligue des Droits de l'Homme v Belgium* (dec.), nos. 32200/96 and 32201/96, ECHR 1998, para 97.
[65] Clare Garvie, Alvaro Bedoya, Jonathan Frankle, 'Perpetual Line-Up: Unregulated Police face Recognition in America' (Georgetown Law Centre on Privacy & Technology, 18 October 2016) <https://www.perpetuallineup.org/risk-framework> accessed 14 February 2019.
[66] Woods, 'Automated Number Plate Recognition' *supra* n 38, 2.
[67] Atockar, 'Riding with the Stars: Passenger Privacy in the NYC Taxicab Dataset' (Neustar Research, 15 September 2014) <https://research.neustar.biz/2014/09/15/riding-with-the-stars-passenger-privacy-in-the-nyc-taxicab-dataset/> accessed 14 February 2019.
[68] ICO, 'Blog: facial recognition technology and law enforcement' (Information Commissioner's Office, 15 May 2018) <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/05/blog-facial-recognition-technology/> accessed 14 February 2019.
[69] EFF, 'Street-level Surveillance' (Electronic Frontier Foundation, undated) <https://www.eff.org/pages/face-recognition> accessed 14 February 2019.
[70] Surveillance Camera Commissioner, 'Working together on automatic facial recognition' (Surveillance Camera Commissioner, 10 October 2018) <https://videosurveillance.blog.gov.uk/2018/10/10/working-together-on-automatic-facial-recognition/> accessed 14 February 2019.
[71] Steve Robson, 'Greater Manchester Police monitored every visitor to Trafford Centre for six months using controversial technology until they were told to stop' (Manchester Evening News, 14 October 2018) <https://www.manchestereveningnews.co.uk/news/greater-manchester-news/gmp-trafford-centre-camera-monitored-15278943> accessed 15 February 2019.
[72] *Herbecq supra* n 64, para 94.

CCTV in cities;[73] in universities and colleges staff[74] and students[75] may avoid discussing contentious topics if they feel under surveillance. Such results, whether intended or not, are a particularly serious problem for institutions that are required by law to protect lawful free speech by their members and visitors.[76]

The senses and risk levels in Table 1 below can also be viewed in terms of human rights. Level 0 is unlikely to represent any threat to those rights; Levels 1 and 2 will engage the rights to privacy and data protection; Levels 3 and 4 may require consideration of other rights, such as free speech and free assembly, as well.

		Sense		
		Location	Audio	Video
Risk Level	0. Presence	Wifi/bluetooth activity	Sound level	Motion sensor
	1. Counting	Wifi/Bluetooth queue monitors		
	2. Identifying			Monitored CCTV
	3. Recording	Logfiles/Access Cards	Audio recording	Video recording
	4. Analysing	Relationship mapping	Voice recognition/ trigger words	ANPR/Face recognition

Table 1 - Senses and risk levels on the intelligent campus

Risks of creep

A particular challenge of intelligent campus applications is that installations may well have unintended and unexpected capabilities. Most of these issues arise in the smart city context but the nature of the campus emphasises them. Campuses (or at least their infrastructure) are used 24 hours a day by students and staff, often functioning as both 'work' and 'home' on far-from-routine timetables. Individuals interact with campus infrastructures in a particularly intense fashion, leaving rich data trails through their use of wireless networks, virtual learning and research environments. Compared to smart cities, an intelligent campus infrastructure is more likely to be controlled by a single organisation: this can offer a single point of organisational ethical control over systems and data or, conversely, create an increased risk of inappropriate combination and use.

Whether in smart cities or intelligent campuses, many sensors are capable of operating at different levels of intrusiveness. As the Commission's draft *ePrivacy Regulation* notes, the same 'scanning of equipment related information' can be used for many purposes and '[w]hile some of these functionalities do not entail high privacy risks, others do, for example, those involving the tracking of individuals over time, including repeated visits to specified locations'.[77] Thus, for example, a microphone installed to measure audio level (Level 0) could also be the source for a Level 4 speech recognition application. Bluetooth sensors used to measure the number of devices present (Level 0) could also be used for real-time analysis

[73] Edwards, 'Privacy, Security and Data Protection in Smart Cities' *supra* n 11, 58.

[74] Leonie Maria Tanczer, Ryan McConville, Peter Maynard, 'Censorship and Surveillance in the Digital Age: The Technological Challenges for Academics' (2016) 4(1) Journal of Global Security Studies 346, 349.

[75] Julie Cupples, 'Default lecture capture: In defense of academic freedom, safety and well-being' (27 August 2018) <https://juliecupples.wordpress.com/2018/08/27/default-lecture-capture-in-defense-of-academic-freedom-safety-and-well-being/> accessed 14 February 2019.

[76] Education (No.2) Act 1986, s.43.

[77] Proposal for a Regulation on Privacy and Electronic Communications, *supra* n 53, Recital 25.

of movement and identification of suspicious patterns (Level 4). Live CCTV (Level 2) may require no more than a software change to implement continuous face recognition (Level 4). This possibility of 'sensor creep' should be borne in mind when designing intelligent campus installations and a be particular focus of risk assessment when existing sensors are re-used for a new purpose.[78] Sensor creep can also occur through careless or malicious activity – for example when baby monitors[79] or ANPR systems[80] are not secured – or when sense data is combined with other information, for example when the owner of a previously pseudonymous device logs in to the wifi network.

Campuses involve a complex mixture of spaces that their occupants are likely to perceive as 'public' or 'private'. The same sensor infrastructure may well cover both: for example libraries and offices; social spaces and accommodation. The Information Commissioner has long advised that CCTV placement should avoid private spaces.[81] Since all senses can be equally intrusive, the same should apply to audio and location, but this may be a greater challenge as both these senses may penetrate through video-opaque walls between public and private spaces. Campuses also contain spaces – such as counselling or medical services and some laboratories – where an individual's presence, either once or regularly, could constitute special category or otherwise high-risk information.

Spaces may even change in nature during the course of a day or term: like the Information Commissioner's concerns about continuous recording in vehicles that functioned as both taxis and family transport,[82] the same campus meeting room may also vary in sensitivity between an open meeting that is intended to be remotely visible and audible and a disciplinary hearing that should definitely not be.

The possibility of creep is also likely to affect individuals' perception of whether an intelligent campus sense is being used acceptably. Attitudes, and possibly behaviour, are likely to be set by the most intrusive use (or perceived use) of each sense. If individuals are concerned that their wifi signals are being used to track them, they may switch to aeroplane mode or refuse to connect to the network, and thereby lose out on location-based assistance. This may also cause significant risks to organisations, for example if staff or students are concerned about secondary uses of swipe card data they may swap cards, thus harming both the secondary purpose and the primary one of enforcing the organisation's physical security policy.

Since many of these effects arise from individuals' perception of risk and benefit, as much as the actual risk and benefit, organisations need both to manage the actual risks and to ensure they are perceived as acceptable. The following sections suggest how that might be done.

---

[78] Surveillance Camera Commissioner, supra n 59, 2.

[79] Kashmir Hill, 'Hackers breaking into baby cams are actually trying to help' (Splinter, 4 July 2015) <https://splinternews.com/hackers-breaking-into-baby-cams-are-actually-trying-to-1793846901> accessed 14 February 2019.

[80] Cooper Quintin and Dave Maass, 'License Plate Readers Exposed! How Public Safety Agencies Responder to Major Vulnerabilities in Vehicle Surveillance Tech' (Electronic Frontier Foundation, 28 October 2015) <https://www.eff.org/deeplinks/2015/10/license-plate-readers-exposed-how-public-safety-agencies-responded-massive> accessed 14 February 2019.

[81] ICO, 'In the picture: A data protection code of practice for surveillance cameras and personal information' (Information Commissioner's Office, 2017), 25 <https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf> accessed 14 February 2019.

[82] ICO, 'Blog: Continuous CCTV in taxis – where do councils stand?' (Information Commissioner's Office, 14 August 2018) < https://ico.org.uk/about-the-ico/news-and-events/blog-continuous-cctv-in-taxis-where-do-councils-stand > accessed 14 February 2019.

Intelligent Campus Risk Management

Before proceeding with a particular intelligent campus application, the organisation should therefore understand the risks it presents and ensure that occupants are likely to consider them acceptable. If not, they may change their behaviour, the organisation's reputation may be harmed, or legal action may even result. The risk levels discussed in the previous section suggest the degree of risk mitigation likely to be needed. Particularly at the higher risk levels, however, the nature of the application's benefits may also be significant in determining whether or not occupants will accept it.

Aion et al identify six groups of intelligent campus applications:

- Learning – applications that 'directly affect the student's ability to learn and succeed';
- Management – managing campus infrastructure and conducting day-to-day operations;
- Social – applications that 'facilitate internal and external collaboration';
- Governance – to provide 'institutional accountability to stakeholders and help enhance its reputation';
- Environmental – ensuring 'efficient use of natural resources ... protect[ing] the environment';
- Health – providing 'proactive, preventive healthcare services'.[83]

These groups clearly involve different kinds of benefits, and to different entities: 'learning' directly benefits the individual; 'governance' indirectly benefits the organisation. Comments from regulators and courts support the possibility that these may result in different levels of risk being acceptable. In its 2014 Opinion on the Internet of Things the Article 29 Working Party suggested that processing data relating to 'location and many other aspects of … private life … will hardly be justified by merely the economic interest which an IoT stakeholder has in that processing. Other interests pursued by the controller or ... third parties … must come into play'.[84] A further subdivision of those 'other interests' is suggested in *Tele2/Watson* where the European Court of Justice distinguishes an 'objective of general interest' (in that case fighting crime) from actions that directly benefit individuals.[85] Applying this to the intelligent campus, we might expect individuals to accept fewest risks where an application serves only the interest of the organisation or a third party; perhaps more for applications – such as environmental efficiency or identifying recent contacts of someone diagnosed with a contagious disease – that benefit a general societal interest; and be most tolerant of risk where an application – such as campus navigation or learning support – directly benefits them.

Data Protection law's concept of purpose compatibility further suggests that individuals may be less tolerant of risk if they perceive a significant distance between the purpose for which information is being used and the purpose for which it was collected. Expectations may derive both from the specific context in which data were collected, and the more general relationships between an educational institution and its students, staff and visitors. If data are

[83] Nora Aion, Linda Helmandollar, Minuuan Wang, Jason W.P. Ng, 'Intelligent Campus (iCampus) Impact Study) (2012) IEEE/WIC/ACM International Conferences on Web Intelligence and Intelligent Agent Technology 291 <http://dx.doi.org/10.1109/WI-IAT.2012.261> accessed 14 February 2019.

[84] Article 29 Working Party, 'Opinion 8/2014 on Recent Developments on the Internet of Things' (2014) 14 EN WP 223, 15.

[85] *Tele2/Watson supra* n 41 paras 94 & 103.

used in an 'unexpected or surprising' way then individuals are likely to object, even to uses that may benefit them.[86]

Risk mitigation

Mitigation measures are always important to reduce risk and to ensure it stays at the intended level. This may be enough to justify a particular intelligent campus application in law. But in intelligent campuses mitigations are also important in building individuals' trust in the system and its operator. Clear, effective and transparent risk management should mean both the organisation and the occupants are comfortable with the intelligent campus.

Many of the risk mitigations applicable to intelligent campus systems are common to all complex data processing systems: Edwards mentions collection minimisation, encrypted dataflows, anonymisation, just-in-time privacy notices, retention periods, user-friendly privacy controls and defaults;[87] the Article 29 RFID guidance highlights governing practices, individual access & control, system protection measures, device protection and accountability measures.[88] Intelligent campus sensors may be particularly attractive targets for malicious attackers – both inside and outside the organisation – wishing to use security cameras and other sensors to remotely monitor the premises, so technical and organisational measures will be particularly important to protect sensors, back-end systems and the communications and data that pass between them.[89]

More specific to the intelligent campus are measures to protect against the various types of 'creep' discussed above: data creep, sensor creep and space creep. In each case, both technical and organisational measures are likely to be needed.[90]

Preventing inappropriate use or combination of data is likely to require organisational and policy measures.[91] If an organisation is using pseudonymous tracking of wireless devices, for example, policy (if possible backed by technical controls) will be the main way to prevent those data being depseudonymised by linking to data from logins on those devices. Similarly, for desk occupancy data to remain anonymous they must be kept separate from data linked to network sockets attached to the desks.

System architecture can play a role: for example in Alqahtani's augmented reality app each mobile device knows its location and requests relevant information from a server.[92] Though this server could track the movement of a device over time it does not need to do so, unlike an alternative design where the server would choose the information based on continuous location and movement information from the device. In a privacy-protecting design, the server should anonymise the requests it makes to third-party services, thus preventing those from tracking individual users as well.

---

[86] Article 29 Working Party, 'Opinion 3/2013 on Purpose Limitation' (2013) 00569/13/EN WP 203, 24.

[87] Edwards, 'Privacy, Security and Data Protection in Smart Cities' *supra* n 11, 50.

[88] Article 29WP, 'RFID Annex' *supra* n 44, Annex IV.

[89] ENISA, 'Good Practices for Security of Internet of Things in the context of Smart Manufacturing' (ENISA, 2018) <https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot> accessed 14 February 2019.

[90] Edwards, 'Privacy, Security and Data Protection in Smart Cities' *supra* n 11, 39.

[91] Article 29WP, 'RFID Annex' *supra* n 44, 18.

[92] Hamed Alqahtani, Manyola Kavalaki, "iMAP-CampUS: Developing an Intelligent Mobile Augmented Reality Program on Campus as a Ubiquitous System" (2017) ACM Proceedings of the 9th International Conference on Computer and Automation Engineering <http://dx.doi.org/10.1145/3057039.3057062> accessed 14 February 2019.

Mobile apps that process sense data locally are better placed to provide effective controls against sensor creep, for example by only enabling sensors at times when they are required for an active app or function, and by respecting 'do-not-disturb' times that the user has set across the device. In addition to these privacy-by-design features, apps should, of course, offer clear information and controls to their users as well as genuine choice whether and when to install or remove them.

Where new sensors are being added to the campus infrastructure, these should be chosen to reduce the risk of unintended data collection. For example it is safer to measure room occupancy with a heat or motion sensor than by post-processing a full-function CCTV camera. Sensor creep can also be reduced by an appropriate choice of reference data: Georgetown University contrast the precisely-targeted face recognition involved in a passport check – which knows nothing about anyone other than the passport-holder – with the general privacy breach involved in comparing a crowd against a driving licence database. [93] The latter will identify many people who are not relevant to the purpose of processing and is much more likely to mis-identify individuals given the much larger number of possibilities available: face recognition software found matches for 28 members of the US Congress in a collection of 25000 mugshots.[94]

Intelligent campuses, in particular, must also develop policies to handle locations and times where sound, vision or location data may be particularly hazardous. Particular care should be taken in areas that occupants may consider 'private', such as accommodation or offices. Though some privacy measures can be provided by careful sensor placement (see, for example, the ICO's guidance on CCTV positioning[95]) the permeability of physical boundaries to sound and location means these should not be relied upon. Data collected from, or near, these areas may need additional access controls and authorisation processes, technical obfuscation or exclusion from algorithmic training and processing, for example.

Transparency

Finally, transparency about intelligent campus activities is essential: not as a risk mitigation but to avoid risk aggravation. Individuals used to being regarded by companies and governments as 'oil'[96] or 'silkworms'[97] may naturally expect the worst: that all data, sensors and systems are re-used for secondary purposes, with even primary purposes being concealed within long legalistic texts.[98] Such activities are likely to be resented, even where data collection and processing would have been accepted if clearly explained in advance. Clear statements of what will be done, why, and under what safeguards, are a good way to demonstrate that intelligent campus practice is different from those precedents.

One practical challenge is to provide such information not just to staff and students, but to those who may simply cross the campus or use its visitor facilities.[99] Signage – as used for

---

[93] Garvie, Bedoya and Frankle, 'Perpetual Line-Up' *supra* n 65.

[94] Sam Levin, 'Amazon face recognition falsely matches 28 lawmakers with mugshots, ACLU says' (Guardian, 26 July 2018) <https://www.theguardian.com/technology/2018/jul/26/amazon-facial-rekognition-congress-mugshots-aclu> accessed 14 February 2019.

[95] ICO, 'Code of practice for surveillance cameras' *supra* n 81.

[96] Meglena Kuneva, (2009) 'Keynote Speech: Roundtable on Online Data Collection, Targeting and Profiling' (31 March 2009) <http://europa.eu/rapid/press-release_SPEECH-09-156_en.htm> accessed 14 February 2019

[97] Ian Brown, Christopher Marsden, *Regulating Code: Good Governance and Better Regulation in the Information Age* (1st edn, MIT Press 2013), 184.

[98] Samson Esayas, 'Competition in (data) privacy: "zero"-price markets, market power and the role of competition law' (2018) 8(3) International Data Privacy Law 181, 190.

[99] Edwards, 'Privacy, Security and Data Protection in Smart Cities' *supra* n 11, 42.

CCTV[100] and wifi tracking[101] – is likely to be required where these individuals may come within reach of the campus's video, audio or location sensors. Such notices are also a useful reminder to staff and students that data may be collected even without conscious action on their part.[102]

A dispute over desk occupancy monitoring highlights several of the issues.[103] The devices used appear to have been passive infra-red (PIR) sensors, which would normally fall into the least intrusive category (Level 0, Presence) as being incapable of gathering personal data.[104] However at least some of the monitored locations were 'personally assigned desks in locked offices', effectively creating a Level 3 Recording Location application. Occupants may also have considered these offices to be private spaces, where sensors were particularly inappropriate. Finally, it is clear that occupants felt they had not received the appropriate level of transparency.

Intelligent Campus Ethics

Risk management may tell us **how** to conduct a particular intelligent campus activity. However the range of potential objectives and data sources requires a more fundamental framework, to guide **which** intelligent campus opportunities we should pursue. This is particularly important in an area where, according to the UK Cabinet Office, '[p]ublic attitudes to data are changing' and '[w]orking with data in a way which makes the public feel uneasy … could put your project at risk and also jeopardise other projects'.[105] Sentiment towards an Intelligent Campus could easily be influenced by objectionable developments elsewhere: Finch and Tene consider '[i]t is not yet clear to which brave new world smart cities will lead us';[106] Edwards notes the risk that 'a significant number of users in smart cities refuse, say, to engage with services provided via smart devices or environments...';[107] the European Data Protection Supervisor detects a 'worrying drift towards thinking that with regards to personal information, whatever is possible is also desirable'.[108]

These concerns in related fields may, however, present an opportunity for Intelligent Campuses to distinguish themselves from wider trends. They could respond to Galdon-Clavell's 'pressure to develop privacy-enhancing smart technologies and privacy-protecting regulatory frameworks'[109] or Finch and Tene's opportunity to 'be part of a framework that engenders trust, empowers urban populaces, and creates new value through

---

[100] ICO, 'Code of practice for surveillance cameras' *supra* n 81, 37.
[101] ICO, 'Wi-Fi location analytics' (Information Commissioner's Office, 2016), 6 <https://ico.org.uk/media/for-organisations/documents/1560691/wi-fi-location-analytics-guidance.pdf> accessed 14 February 2019
[102] Edwards, 'Privacy, Security and Data Protection in Smart Cities' *supra* n 11, 42.
[103] Catriona Stewart, 'Glasgow Unversity staff apologise after "tracking students"' (Evening Times, 17 May 2017) <https://www.eveningtimes.co.uk/news/15292214.glasgow-university-staff-apologise-after-tracking-students/> accessed 14 February 2019.
[104] OccupEye, 'How it works' (OccupEye, undated) <https://www.occupeye.com/how-it-works/> accessed 14 February 2019.
[105] Cabinet Office, 'Data Science Ethical Framework (Version 1.0)' (UK Government, 19 May 2016), 3 <https://www.gov.uk/government/publications/data-science-ethical-framework> accessed 14 February 2019.
[106] Finch and Tene, 'Welcome to the Metropticon' *supra* n 9, 1615.
[107] Edwards, 'Privacy, Security and Data Protection in Smart Cities' *supra* n 11, 58.
[108] Giovanni Buttarelli, 'Big data, big data protection: challenges and innovative solutions' (Keynote speech to ERA Conference on Recent Developments in Data Protection Law, 11 May 2015) <https://edps.europa.eu/sites/edp/files/publication/15-05-11_era_speech_en.pdf> accessed 14 February 2019.
[109] Galdon-Clavell, '(Not so) smart cities?' *supra* n 10, 718.

personalisation'.[110] The Cabinet Office proposes ethics as the guide to this confidence-building path: 'law tells us what we can do, but ethics tells us what we should do. Ethics become more important when advances in technology are pushing our understanding of the law to its limits.'[111]

Kitchin identifies six ethical concerns for smart cities:

1. Datafication, dataveillance and geosurveillance
2. Inferencing and predictive privacy harms
3. Anonymisation and re-identification
4. Obfuscation and Reduced Control
5. Notice and Consent Empty or Absent
6. Data Use, Sharing & Repurposing[112]

This section considers how two ethics codes – the UK Government's 2016 Data Science Ethical Framework (in the following, 'DSEF') and the Menlo Report's Ethical Principles for ICT Research ('Menlo') – can help us address those concerns. The DSEF was designed to 'give[] those analysing or making policy or operational decisions with data the confidence to operate. It balances the use of new data and techniques with respect for privacy and makes sure no-one suffers *unintended* negative consequences'[113] (its 2018 revision is much more specific to the central government context, so less useful elsewhere[114]); Menlo applies long-established ethical principles for human behaviour research to research on Information and Communication Technologies (ICT) that have 'increasingly become integrated into our individual and collective daily lives, mediating our behaviours and communications'.[115]

1. Datafication, dataveillance and geosurveillance

Kitchin considers it 'all but impossible to live everyday lives without leaving digital footprints (traces we leave ourselves) and shadows (traces captured about us)'.[116] His examples include many of the technologies likely to be present on Intelligent Campuses: CCTV (including image processing); bluetooth/wifi tracking; smart card tracking; mobile phone tracking; tracking devices, whether imposed by courts or family members; ATMs, credit card purchases, library loans, geotagged photos and tweets.[117] This results in 'a situation where the monitoring of location is pervasive, continuous, automatic and relatively cheap and it is relatively easy to construct travel profiles and histories'.[118]

From this data deluge, the Intelligent Campus operator must not only practise restraint in the selections it makes, it must also demonstrate that it is doing so. The DSEF's Principle 2 requires careful choices: 'Use data and tools which have the minimum intrusion necessary', 'Only use personal data if similar insight or statistical benefit cannot be achieved using non-

[110] Finch and Tene, 'Welcome to the Metropticon' *supra* n 9, 1606.
[111] Cabinet Office, 'Data Science Ethical Framework' *supra* n 105, 14.
[112] Kitchin, 'The ethics of smart cities and urban science' *supra* n 13, 5-10.
[113] Cabinet Office, 'Data Science Ethical Framework' *supra* n 105, 3 .
[114] Cabinet Office, 'Data Ethics Framework' (UK Government, 13 June 2018) <https://www.gov.uk/government/publications/data-ethics-framework> accessed 14 February 2019.
[115] 'The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research' (Homeland Security Science and Technology, 3 August 2012), 5 <https://www.dhs.gov/sites/default/files/publications/CSD-MenloPrinciplesCORE-20120803_1.pdf> accessed 14 February 2019.
[116] Kitchin, 'The ethics of smart cities and urban science' *supra* n 13, 6.
[117] Kitchin, 'The ethics of smart cities and urban science' *supra* n 13, 8.
[118] Kitchin, 'The ethics of smart cities and urban science' *supra* n 13, 6.

personal data', and 'De-identify individuals or aggregate to higher geographical levels where possible'.[119]

Both DSEF Principle 5 and Menlo Principle 4 require transparency: 'Aim to be publicly transparent about what you are doing and be open about the tools, data and algorithms used and its intention … provide your explanations in plain English'[120] and '[Transparency] also involves clear communication of risk assessment and harm minimization related to research activities.'[121] DSEF regards transparency as providing self-discipline: 'It is also good antiseptic for unethical behaviour'.[122] Menlo sees it as an essential corrective in novel situations that challenge more traditional controls:

> Transparency and accountability serve vital roles in many [] contexts where it is challenging or impossible to identify stakeholders [], to understand interactions between highly dynamic and globally distributed systems and technologies, and consequently to balance associated harms and benefits.[123]

The Framework's conclusion seems equally applicable to Smart Cities and Intelligent Campuses: 'A lack of transparency and accountability risks undermining the credibility of, trust and confidence in, and ultimately support for, ICT research.'[124]

2. Inferencing and predictive privacy harms

Kitchin sees two ethical issues with using algorithms to generate new information from observed data: that algorithms might infer information – whether accurate or not – that an individual wishes to keep secret, and that actions may be taken based on inaccurate inferences. Both smart cities and intelligent campuses can have a broad impact across their occupants' lives so revealed secrets and errors can cause widespread harm: '[s]uch inferences can generate inaccurate characterization that then stick to and precede an individual'.[125]

DSEF principle 3 deals directly with Robust Data Science Models, setting requirements before, during, and after processing. Proposed inputs must be checked for 'limits and opportunities of data': 'errors or bias in input data', 'who the data is representative of'; algorithms must be checked to ensure they do not generate discriminatory proxies for protected characteristics and there must be 'procedures in place so you can tell when something has gone wrong and … a process for fixing it'; any output must be accompanied by 'an accuracy rating for the insight so that people can decide how to use it' and the provenance of insights from elsewhere must be understood. In addition to these tests of algorithms, the intended outcomes must be checked to determine 'whether an incorrect decision will have unintended negative consequences for someone or distress someone, and if there is a risk – whether the public benefit justifies this'.[126] The UK Information Commissioner's concerns about face recognition technology, discussed above, raise all these issues.[127]

---

[119] Cabinet Office, 'Data Science Ethical Framework' *supra* n 105, 9.
[120] Cabinet Office, 'Data Science Ethical Framework' *supra* n 105, 15.
[121] Menlo Report *supra* n 115, 16.
[122] Cabinet Office, 'Data Science Ethical Framework' *supra* n 105, 15.
[123] Menlo Report *supra* n 115, 15.
[124] Menlo Report *supra* n 115, 15.
[125] Kitchin, 'The ethics of smart cities and urban science' *supra* n 13, 8.
[126] Cabinet Office, 'Data Science Ethical Framework' *supra* n 105, 11-12.
[127] ICO, 'Blog: facial recognition technology and law enforcement' *supra* n 68.

Neither the DSEF nor Menlo mention the 'right to an explanation', which may apply to some algorithmic processing under the GDPR.[128] Edwards and Veale conclude that such rights are not sufficient to avoid unfairness – both because they aim to repair, rather than prevent, harm and because individuals may lack the resources to exercise them – and that we need measures that 'have impacts upstream, while systems are being designed or at least before they are deployed'.[129] An ethical Intelligent Campus must aim to have its algorithms make good decisions in the first place, rather than relying on individuals' ability to challenge bad ones.

3. Anonymisation and re-identification

Kitchin observes that true anonymity is hard to ensure in an environment that collects as much data as a smart city. So long as data are recorded about individuals, it is possible that patterns in those data may be sufficient to identify them, if not by name then by a unique pattern of behaviour. More directly, some claims of 'anonymity' in fact relate to systems that are designed to provide a personalised experience: '[t]he term "anonymous identifier", as used by some companies … is thus somewhat of an oxymoron, especially when the identifier is directly linked to an account with known personal details.'[130]

The DSEF notes the importance of managing the linking and anonymisation processes, giving the example of Administrative Data Research Network '"safe havens" where administrative data … can be anonymised and linked, with strict controls for who has access for the data and for how long'.[131] Rather than considering anonymisation as a one-off process that removes all future risk, it is better to recognise anonymisation, de-identification and pseudonymisation as measures that reduce risk but do not eliminate it.[132] Finch and Tene agree that '[w]hile de-identification can no longer be treated as a "silver bullet," de-identified data sets still provide significant social utility with lowered privacy risks.'[133]

According to the UK Anonymisation Network, 'accepting that there is a residual risk in all useful data inevitably puts you in the realms of balancing risk and utility'.[134] That risk can only be assessed in the context of a particular 'data environment',[135] and that environment may change over time as new datasets, tools, or motivations for data misuse emerge. Management of data – whether personal, anonymised, or neither – must be treated as an ongoing process of both risk management and decision making: are current uses of data still safe? are proposed new uses acceptable?[136]

4. Obfuscation and reduced control & 5. Notice and consent empty or absent

Probably the most challenging aspect of the Intelligent Campus for traditional ethics approaches is the lack of individual control over data collection and processing. Individuals cannot avoid using the infrastructures – buildings, spaces, access controls, networks, etc. – from which information is gathered, so have 'little choice in being surveilled'.[137] Much of

---

[128] Lilian Edwards, Michael Veale, 'Enslaving the Algorithm: From a Right to an Explanation to a "Right to Better Decisions"?' (2018) 16(3) IEEE Security & Privacy 46, 46-48.

[129] Edwards and Veale, 'Enslaving the Algorithm' *supra* n 128, 50.

[130] Kitchin, 'The ethics of smart cities and urban science' *supra* n 13, 8.

[131] Cabinet Office, 'Data Science Ethical Framework' *supra* n 105, 17.

[132] Mark Elliot, Elaine Mackey, Kieron O'Hara and Caroline Tudor, 'The Anonymisation Decision-Making Framework' (UKAN/University of Manchester, 2016), 1 <http://ukanon.net/wp-content/uploads/2015/05/The-Anonymisation-Decision-making-Framework.pdf> accessed 14 February 2019.

[133] Finch and Tene, 'Welcome to the Metropticon' *supra* n 9, 1612.

[134] Elliot et al, 'Anonymisation Framework' *supra* n 132, 5.

[135] Elliot et al, 'Anonymisation Framework' *supra* n 132, 2.

[136] Elliot et al, 'Anonymisation Framework' *supra* n 132, 2.

[137] Kitchin, 'The ethics of smart cities and urban science' *supra* n 13, 9.

this information gathering occurs during routine, continuous use of those infrastructures: there are few discrete transactions where individuals might be informed or reminded of the data being collected and the uses to which they are being put.[138] Retrospective controls such as objection or individual data access may also be hard to implement – it is 'simply too onerous for individuals to police their privacy'[139] – while privacy-protecting data flows mean individuals must breach their own privacy, and perhaps that of others, to exercise these rights. For example, a request to be obscured from CCTV requires a human to watch the whole recording, which might otherwise have remained confidential. As noted above, Intelligent Campuses normally involve simpler organisational structures than smart cities, so organisational accountability and control should be less of a problem.[140]

While Menlo's first principle – Respect for Persons – is normally achieved through informed consent, the Code recognises that, even in the research context, this may not be possible to obtain: 'In such situations, respect for persons is maintained by … instead focusing on data protections and/or removal of identifying information that is not germane to research as alternative means of minimizing potential harm'.[141] To be permissible without consent, the organisation must ensure that its conduct creates 'no more than minimal risk' to individuals, that their 'rights and welfare' will not be adversely affected, that the activity 'could not practicably be carried out' in any other way, and 'whenever appropriate, the subjects will be provided with additional pertinent information after participation'.[142]

There is a growing belief that this approach, placing responsibility on organisations, should no longer be seen as second-best to prior individual consent. Particularly in the on-line environment, the quantity and complexity of data processing make it impractical for individuals to make informed decisions about what is done with their personal data: they 'have neither the resources, opportunity, inclination, or motivation' to do so.[143] In many cases, according to Edwards and Veale '[c]onsent has become a formality validating the actions of the data controller rather than something empowering the user'.[144] Even where meaningful consent appears to be possible 'the way forward may simply be to admit that consent is only a first step to lawful processing and that regardless of such permission, certain uses of that data, on the environmental model, are toxic and thus prohibited'.[145]

If 'responsibility for ensuring ethical and responsible data collection should be on the data collectors, not the hapless users',[146] then Menlo's four tests should, perhaps, be applied to all intelligent campus activities. Campus occupants should still be offered choices where these are meaningful: for example by implementing campus navigation tools as location-aware apps that users can chose when to install and enable, rather than as services that continually track location, or by seeking "downstream consent" at the point when the implications of personalisation can be clearly set out.[147] But even systems where users do have a free choice

[138] Edwards, 'Privacy, Security and Data Protection in Smart Cities' *supra* n 11, 42.
[139] Kitchin, 'The ethics of smart cities and urban science' *supra* n 13, 9.
[140] Kitchin, 'The ethics of smart cities and urban science' *supra* n 13, 9.
[141] Menlo Report *supra* n 115, 11.
[142] Menlo Report *supra* n 115, 11.
[143] Edwards, 'Privacy, Security and Data Protection in Smart Cities' *supra* n 11, 55.
[144] Edwards and Veale, 'Enslaving the Algorithm' *supra* n 128, 50.
[145] Edwards, 'Privacy, Security and Data Protection in Smart Cities' *supra* n 11, 56.
[146] Edwards, 'Privacy, Security and Data Protection in Smart Cities' *supra* n 11, 56.
[147] Andrew Cormack, 'Downstream Consent: A Better Legal Framework for Big Data' (2016) 1(1) Journal of Information Rights, Policy and Practice.

should be designed, implemented and operated according to an ethical framework. Any hint of 'consent as formality' or forcing individuals to make impossible choices must be avoided.

The first three Menlo tests are strikingly similar to those involved in a Data Protection Impact Assessment (DPIA), set out in Article 35(7) of the General Data Protection Regulation. That process makes a further ethical contribution, by recommending that 'where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing'.[148] Since a DPIA is designed as a cyclic process[149] it could involve campus users in decisions on the purposes and data chosen for intelligent campus projects, the safeguards incorporated, and an ongoing review of the risks and benefits that result from the activity. Such a review might well be an opportunity to provide the 'additional pertinent information' recommended by the fourth Menlo test. Where prior consensus can be achieved among both campus users and operators on the design, implementation and continuing operation of intelligent campus systems, the risks from lack of retrospective individual control should be significantly reduced.

6. Data use, sharing and repurposing.

Kitchin is concerned that the purposes for which smart city data are used often go well beyond what their occupants would expect: 'few of those whose data have fed into creating predictive profiles imagined that their data were going to be repurposed to social sort or regulate or control them, or nudge them towards certain behaviours'.[150] Such problems may arise both at the initial design stage and through subsequent evolution of data and systems, with 'data and services … used to perform a wide variety of tasks for which the data were never intended'.[151]

Research ethics codes respond to these concerns in two ways: choosing appropriate topics for research and being transparent about its purpose and benefits. Thus the first DSEF principle is to 'Start with clear user need and public benefit';[152] Menlo's Beneficence principle requires that 'researchers should identify benefits and potential harms from the research for all relevant stakeholders, including society as a whole, based on objective, generally accepted facts or studies',[153] and stresses that 'researchers [not reviewers or Ethics Boards] bear the burden of illuminating those risks and their consideration of how those risks will be managed';[154] DSEF Principle 5 requires that researchers '[l]et people know about the social benefit of your work and the impact it has had on collective or individual social or financial outcomes'.[155]

Smart city commentators agree that topic choice and transparency are necessary – for example Galdon-Clavell: '[r]esponsibility involves the attempt to achieve socially desirable outcomes'[156] – but suggest these may not be sufficient. Finch and Tene observe that 'smart city technologies also introduce the potential for much more individualistic paternalism - potentially allowing cities to 'protect' citizens from themselves', for example a Fitbit-

[148] *General Data Protection Regulation supra* n 20, Article 35(9).
[149] ICO, 'Data Protection Impact Assessments' (Information Commissioner's Office, undated) <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/> accessed 14 February 2019.
[150] Kitchin, 'The ethics of smart cities and urban science' *supra* n 13, 10.
[151] Kitchin, 'The ethics of smart cities and urban science' *supra* n 13, 10.
[152] Cabinet Office, 'Data Science Ethical Framework' *supra* n 105, 8.
[153] Menlo Report *supra* n 115, 12.
[154] Menlo Report *supra* n 115, 13.
[155] Cabinet Office, 'Data Science Ethical Framework' *supra* n 105, 15.
[156] Galdon-Clavell, '(Not so) smart cities?' *supra* n 10, 721.

connected escalator could switch off to help particular individuals get more exercise.[157] They comment 'such intentions are surely noble, they are also paternalistic and could quickly become oppressive'.[158]

Kitchin hints at a further guide: 'data repurposing can break what is considered compatible forms of data re-use and the reasonable expectations of data subjects'.[159] While purpose compatibility and reasonable expectations are familiar as legal terms, the word 'considered' applies them to a different realm: how citizens conceive the spaces they occupy. Mere beneficence and transparency cannot change this. Indeed DSEF Principle 4 requires that researchers 'be alert to public perceptions': treating them as an external factor that may well be influenced by events – such as bad practice elsewhere – that are outside the project's control. Thus the ethical requirement to 'understand both stated and revealed public opinion (people's actual behaviour) about how people would want the data you hold about them to be used … Make sure it is not just you making the decision and that you consult others to work out whether projects are acceptable'.[160]

Intelligent Campus Citizens

Both the Impact Assessment and Ethics analyses therefore propose a new role for the occupants of intelligent campuses. Impact Assessments require that occupants' views be sought on 'intended processing';[161] Ethics requires prior consultation on acceptability. Occupants must be involved before intelligent campus systems are deployed or used for a new purpose, not just afterwards. As discussed in the previous section, four of Kitchin's ethical concerns - Datafication, Dataveillance and Geosurveillance; Inferencing and Predictive Privacy Harms; Anonymisation and Re-identification; Data Use, Sharing & Repurposing – can only be addressed in the design stage; the Menlo Principles suggest that the other two – Obfuscation and Reduced Control and Notice and Consent Empty or Absent – should also be considered before a system is deployed, rather than remedied afterwards. Bernal calls for internet rights to be built into our systems, rather than treating them as fallbacks that individuals can invoke after things go wrong.[162] Giving occupants the ability to select and challenge the purpose, design and implementation of smart spaces, proactively eliminating or mitigating risks to all occupants, seems preferable to merely letting each individual retrospectively manage only their personal risk and harm though rights of information, data access and objection. Achieving consensus on the acceptability of proposals, and then holding organisations accountable for implementing that consensus, should reduce the risks of behaviour change, active resistance and legal or human rights challenges; it also avoids wasting money on systems and purposes that are later found to be unacceptable.

Involving occupants in decision-making and review has further benefits. Leong sees dialogue with citizens contributing to correct interpretation of data: do pedestrians avoid certain streets because they are unsafe, or because they have no shade?[163] Galdon-Clavell's 'mission creep

[157] Finch and Tene, 'Welcome to the Metropticon' *supra* n 9, 1597.
[158] Finch and Tene, 'Welcome to the Metropticon' *supra* n 9, 1598.
[159] Kitchin, 'The ethics of smart cities and urban science' *supra* n 13, 10.
[160] Cabinet Office, 'Data Science Ethical Framework' *supra* n 105, 14.
[161] *General Data Protection Regulation supra* n 20, Article 35(9).
[162] Bernal, *Internet Privacy Rights: Rights to Protect Autonomy supra* n 14, 15.
[163] Mary Leong, 'Why Your Smart City Strategy Needs to Include Citizen Engagement' (PlaceSpeak Blog, 2018) <https://blog.placespeak.com/why-your-smart-city-strategy-needs-to-include-citizen-engagement/> accessed 14 February 2019.

both during the design process and afterwards' might be avoided if occupants were involved in the continuous monitoring of the ways and purposes for which data are processed.[164] Finch and Tene note the benefits of 'reciprocity' where citizens/occupants can themselves use and benefit from the data that are generated.[165] By enabling individuals to develop the apps and services they want, initiatives such as the UK Government's Open Data[166] can both help occupants and demonstrate to campus managers the actual and potential benefits of their investment.

The same relationship – where citizens influence the choice, design, monitoring and use of systems and data – has been the aspiration of smart city theories and initiatives. In De Lang and De Waal's 'ownership' vision, 'urban technologies engage and empower people to become active in shaping their urban environment, to forge relationships with their city and other people, and to collaboratively address shared urban issues'.[167] However this seems hard to achieve in practice. Analysing Dublin's smart city activities against a four-step scale – non-participation, consumerism, tokenism, citizen power – Cardullo and Kitchin found no examples of citizen power and only a few of tokenism.[168] Likewise, in their examination of projects receiving European funds, 'these "citizen-focus" projects score overwhelmingly in the lower categories … with their initiatives realistically offering forms of tokenism (informing or consultation with feedback) or non-participation'.[169] Martin et al similarly found 'substantial evidence of citizens being framed and engaged as users of technological systems',[170] but much less of higher-level engagement in the purpose or design of those systems.

Cardullo and Kitchin identify two reasons for this: that the principal objective of initiatives is often to attract more private funding, rather than more citizen engagement;[171] and that project funding rules require detailed objectives to be set and approved before there is any possibility of citizen consultation on what those objectives should be.[172] An EU-funded project set a target to increase the number of electric vehicles, when citizens actually wanted to decrease the number of cars: its project leader admitted 'there is too wide a gap between how these projects are working and the concerns and issues that real people are facing in their everyday lives'.[173] Where citizens are involved – by 'producing an app or feeding back on a development plan'[174] – this is typically to improve the supplier's ability to manage problems

[164] Galdon-Clavell, '(Not so) smart cities?' *supra* n 10, 721.
[165] Finch and Tene, 'Welcome to the Metropticon' *supra* n 9, 1612.
[166] 'data.gov.uk : Find Open Data' (UK Government, undated) <https://data.gov.uk/> accessed 14 February 2019.
[167] Michiel De Lange and Martijn de Waal, 'Owning the city: new media and citizen engagement in urban design' (2013) First Monday 18(11) <https://firstmonday.org/ojs/index.php/fm/article/view/4954/3786> accessed 14 February 2019.
[168] Cardullo and Kitchin, 'Being a "citizen" in the smart city' *supra* n 22, 5.
[169] Paolo Cardullo and Rob Kitchin, 'Smart urbanism and smart citizenship: The neoliberal logic of "citizen-focused" smart cities in Europe' (2018) Environment and Planning C: Politics and Space, 7 <https://doi.org/10.1177%2F0263774X18806508> accessed 14 February 2019.
[170] Chris J Martin, James Evans, Andrew Karvonen, 'Smart and Sustainable? Five tensions in the visions and practices of the smart-sustainable city in Europe and North America' (2018) 133 Technological Forecasting and Social Change 269, 274.
[171] Cardullo and Kitchin. "Smart Urbanism" *supra* n 169, 9.
[172] Cardullo and Kitchin, 'Being a "citizen" in the smart city' *supra* n 22, 8.
[173] Cardullo and Kitchin. "Smart Urbanism" *supra* n 169, 8.
[174] Cardullo and Kitchin, 'Being a "citizen" in the smart city' *supra* n 22, 10.

such as traffic congestion, not to address the reasons why there is more demand for private transport than the infrastructure can support.[175]

Smart city initiatives seem, therefore, to have fallen well short of the 'ideal city … that guarantees the right for inhabitants to participate fully in the production of urban space',[176] not as mere 'consumers or testers' but being able to 'challenge or replace the fundamental political rationalities shaping an issue or plan'.[177] Cardullo and Kitchin see the need for fundamental change, placing 'citizens and civility … at the core of smart city initiatives, rather than capital and the market'.[178] According to Martin et al, citizens must move from users of tools and spaces prescribed by the city and its suppliers, to full 'participat[ion] in the processes of urban governance'.[179] The only city taking this step appears to be Barcelona, where the Council announces a topic for consideration, then engages in extensive face-to-face and on-line discussion to determine the appropriate mechanism – plan, regulation, or system – to use to improve the current situation.[180] However, Galdon considers even this 'technological sovereignty' to be insufficient. Citizens' powers to protect their rights must be complemented by city managers' guarantees that digital systems behave responsibly and ethically.[181]

This analysis suggests that intelligent campuses may have a much better chance of delivering the right balance between citizen participation and institutional responsibility, to 'enable people to act as co-creators of livable and lively [spaces]'[182] and hold managers accountable for the safe operation of those spaces.[183] Smart city grants may be largely dependent on meeting the formal requirements of national and international competitions, but universities and colleges see current student satisfaction significantly influencing future recruitment and, thereby, income.[184] Whereas smart city projects are often large-scale partnerships with commercial suppliers and integrators, most of the examples identified by Jisc are small-scale and driven by local institutional or individual needs.[185] Cardullo and Kitchin expect to find such bottom-up projects at the top of their scale, with individual involvement in 'ideas, vision, leadership, ownership, create, negotiate, produce'.[186] Finally, with Martin et al identifying 'digital literacy' as a potential barrier to greater participation in cities, campuses should be a good place to find the 'critical mass of digital innovations and motivated citizens' needed to 'prompt a broader transformation of … infrastructure'.[187] Successful intelligent campuses will need both 'citizen engagement and citizen power'[188] and institutional

[175] Cardullo and Kitchin. "Smart Urbanism" *supra* n 169, 10.
[176] Cardullo and Kitchin. "Smart Urbanism" *supra* n 169, 6.
[177] Cardullo and Kitchin, 'Being a "citizen" in the smart city' *supra* n 22, 10.
[178] Cardullo and Kitchin. "Smart Urbanism" *supra* n 169, 13.
[179] Martin et al, 'Smart and Sustainable?' *supra* n 170, 275".
[180] Cardullo and Kitchin. "Smart Urbanism" *supra* n 169, 14.
[181] Gemma Galdon,'Technological Sovereignty? Democracy Data and Governance in the Digital Era' (CCCBLab, Cultural Research and Innovation, 2017) <http://lab.cccb.org/en/technological-sovereignty-democracy-data-and-governance-in-the-digital-era/> accessed 14 February 2019.
[182] De Lang and De Waal 'Owning the City' *supra* n 167.
[183] Jisc, 'The Intelligent Campus' *supra* n 1, 25.
[184] National Student Survey, 'Why Take the survey' (2019) <https://www.thestudentsurvey.com/> accessed 14 February 2019.
[185] Jisc, 'Intelligent Campus: Use Cases' (2018) <https://intelligentcampus.jiscinvolve.org/wp/use-cases/> accessed 14 February 2019.
[186] Cardullo and Kitchin, 'Being a "citizen" in the smart city' *supra* n 22, 5.
[187] Martin et al, 'Smart and Sustainable?' *supra* n 170, 276.
[188] Cardullo and Kitchin, 'Being a "citizen" in the smart city' *supra* n 22, 11.

accountability, throughout their choice, design, implementation and use, if they are to benefit fully from the intelligence and insights of all those who use them.