Original Research Article

BIG DATA & SOCIETY

Big Data & Society
January–June: 1–13
© The Author(s) 2022
Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/20539517221092656
journals.sagepub.com/home/bds
SAGE

Smart campus communication, Internet of Things, and data governance: Understanding student tensions and imaginaries

Pauline Hope Cheong[1] and Pratik Nyaupane[2]

Abstract

In recent years, universities have been urged to restructure and re-evaluate their ability to trace and monitor their students as the "smart campus" is being built upon datafication, while networked apps and sensors serve as the means through which its constituents are connected and governed. This paper advances a dialectical and communication-centered approach to the Internet of Things campus ecosystem and provides an empirical investigation into (a) the tensions experienced by students and (b) the ways that these students envision alternative practices that support their digital engagement. Drawing upon student focus group interviews in a large American research and innovation intensive university, dialectical tensions identified include convenience–annoyance, integration–independence, and safety–insecurity, brought upon by students' ongoing and prospective negotiations with Internet of Things. Furthermore, in a bid to understand students' alternative data imaginaries, this project examined students' preferred Internet of Things-related communication practices with campus digital application platforms, analog and older forms of digital media, as well as in-person interactions with traditional authorities within classroom and group settings. Finally, this contribution presents a discussion of the findings for theory and praxis, particularly for smart campus innovation and social data governance, in terms of potential growing challenges involving complexifying student privacy concerns, data normalization and coercion, and tertiary digital divides and inequalities.

Keywords

Smart campus, internet of things, datafication, data governance, human communication, digital divide

This article is a part of special theme on Social Data Governance. To see a full list of all articles in this special theme, please click here: https://journals.sagepub.com/page/bds/collections/socialdatagovernance

Background and introduction

In the face of expanding communication networks with digitalization, connective devices, and the Internet of Things (IoT), how people experience and navigate the challenges of datafication in their everyday lives is an issue of growing import (Van Dijck, 2014), including the higher educational domain as a key data frontier (Beer, 2019). To many throughout the existence of higher education institutions, university life functions as sanctuaries for learning and an "open door to let hidden talent be uncovered" (Clark, 1963). In democratic countries, universities as key institutions of civil society "have the ability not only to be key arbiters of how one advances democracy, but also to reflect democratic values in their practices, objectives, and goals" (Tierney, 2021: 3). Yet, in recent years and during the unfolding of the global health pandemic, universities in America and worldwide have been urged to restructure

[1]Hugh Downs School of Human Communication, Arizona State University, USA
[2]Annenberg School of Communication and Journalism, University of Southern California, USA

Corresponding author:
Pauline Hope Cheong, Hugh Downs School of Human Communication, Arizona State University, USA.
Email: pauline.cheong@asu.edu

and re-evaluate their ability to trace and monitor student campus-wide and off-campus activity.

In tandem, the growing significance of the "smart campus" is being built upon investment in digital applications and big data practices, while IoT networked apps and sensors serve as the technological and communicative means through which its constituents are connected and governed (Bonderud, 2019; Min-Allah and Alrashed, 2020). "Smart" technology as an acronym refers to self-monitoring, analysis, and reporting technology and is increasingly integrated into everyday environments. However, as smart campus infrastructure development is tuned to resource efficiency, space utilization, and the neoliberal impulse to quantify classroom learning behaviors (Kwet and Prinsloo, 2020), literature on technocentric perspectives and information system management approaches has overshadowed the human dimensions of adopting campus-wide IoT innovations (Prandi et al., 2020). Moreover, competitive conditions within "academic capitalism" along with the reduction in government funding for American academic institutions have resulted in opportunistic collaborations between university administration, external stakeholders, and private industries (Jessop, 2018). While a number of scholars have voiced concerns over institutional asymmetric power and knowledge disparities linked to surveillance capitalism in wider society (e.g. Barassi, 2019; Zuboff, 2019), relatively less attention is being paid to datafication and social data governance in non-profit and educational settings beyond learning analytics, especially considering students' concerns and lived experiences (Vasileva et al., 2018).

This paper advances a dialectical and communication-centered approach to datafication of student activity on the smart campus and provides an empirical investigation into the tensions experienced and ways that students envision alternative practices that support their digital engagement. In doing so, this research extends conceptual understanding of the concurrent communicative benefits and challenges experienced under the conditions of "dataveillance" (Van Dijck, 2014), and "datafied normalization" of students governed within so-called smart and sentient technological systems on campus (Yang and Cole, 2022). Empirical findings also complement growing research that showcases and responds to user-centered needs and experiences, with the case of smart campus initiatives contributing to a more complete picture of the social dimensions of datafication, algorithmic normativity (Grosman and Reigeluth, 2019), and what agency and inclusion mean in a contemporary society. The next section turns to the contemporary debate and literature related to tensions in smart campus life, before moving on to present two research questions, the research methodology, and the discussion of results.

Debates on data practices in hyperconnected campus life

Higher education organizations in the United States and worldwide have been undergoing deep mediatization fueled by new media institutional logics involving standardization, metricization, and connectivity (Rawolle and Lingard, 2014), supported by "always-on" networks to information and people living "hyperconnected lives" (Anderson and Rainie, 2012). Present-day college campuses are outfitted with networked applications and sensors that detect and circulate data, thereby becoming "smart"; yet, this projected "intelligence" raises questions about new forms of human–machine communication that facilitate tracking and surveillance (Bunz and Meikle, 2018).

In recent times, technologically centered visions have taken much of the spotlight in news, which positively portray contemporary campus life. The rise of the titular mycampus app that pushes content and alerts to students on any device has been recognized as vital for driving engagement and retention: "the ultimate hub for on-campus activities or for keeping students unified while remote" (https://www.mobileupsoftware.com/campus-mobile-app/). Latest university partnerships with telecommunications companies to integrate emergency blue light boxes equipped with sensors, augmented reality, and video analytic technologies, college safety apps and smart lightning, have similarly been promoted as augmenting campus security. According to university spokespersons, these technologies encompass a new "mesh environment" with IoT sensors built to provide data on immediate emergency location, identify areas of security and concerns, and enhance safety (Tettlema, 2020). Furthermore, amid the unfolding of the recent pandemic, IoT wearables like "biobuttons" stuck onto the human skin have been rolled out onto American university campuses, with claims to help wearers detect signs of Covid-19 and aid in contact tracing of those infected. These buttons continuously measure temperature, response rate and heart rate, monitor social contacts, and sense user locations (Mangan, 2021). New location tracking apps or existing campus apps paired with Bluetooth sensors in classrooms have been also configured to record students' attendance and movements on and off campus (Whittaker, 2020).

Thus, as smartness is projected onto the educational campus and IoT applications serve to instantiate connected and personalized portal experiences, networked systems are legitimated and prized for maintaining student security, well-being, and community engagement. Yet, these datafication practices pose significant questions not only for university administration but also for users' intrinsic lived experiences amid "datafied normalization" or disciplinary mechanisms to render college students' behavior knowable and governable (Yang and Cole, 2022). Data-ist models of the IoT raise important issues surrounding digital participation, social inclusion, and student privacy rights in particular, and the fair governance of information in the big data era is clear and obvious.

Recent debates and fallout from the implementation of digitalized tools, which students believe to be ineffective, intrusive, and risky, have sparked a resurgence of concerns about mediatizing campus developments. Since the Fall of 2017, successive news stories have featured American universities working with Amazon web services to provide, free to students, the IoT enabled voice-based device Echo Dot, with Saint Louis University being the first to house the technology in every dorm and on-campus apartment (Tate, 2018). In the latter case, as networked devices were configured for "public information" only, students could not reconfigure the settings or tie to their personal accounts to the Dot, significantly limiting user autonomy and access. Tensions with campus networked technologies were also evident where less than a third of students in another university polled by their campus newsletter expressed support for plans to install Echo Dots in dormitories. Students raised concerns about the lack of their input in the university decision-making process to what has been described as "wasteful, impractical and a violation of residents' privacy" (Hobohm, 2019). In the throes of Covid-19, the hurtling of new apps and proctoring tools have heightened awareness about the benefits and challenges of campus-wide monitoring (Shwayder, 2020). News stories have opined that universities are turning into "surveillance machines," highlighting emerging dilemmas from those who have no way to opt out, even from flawed contact-tracing apps with security vulnerabilities (Whittaker, 2020), and poorly functioning and glitchy interfaces (Harwell, 2019).

Related to data governance, questions have also been raised about data protection in remote exam supervision, the normalization of "surveillance creep" and infantilization of students in the hasty implementation of datafied micromanagement (Harwell, 2019), "often with little regard for either its effectiveness or its impact on civil liberties" (Herold, 2019). In one striking case, the "need for a quick turnaround" for the physical installation of small Bluetooth beacons on campus halls and under students' desks resulted in "confusion and chaos" to the point of that a Dean had to order the removal of a beacon off the wall and attributed "a lack of communication" for the panic in the university (Harwell, 2019). Given recent and emerging smart campus developments, it is necessary, therefore, to think much more critically about student encounters with connected devices, particularly tensions they experience as a part of human–machine communication within IoT networks.

Dialectics in IoT campus communication

The focus on IoT communication here deepens mainstream understanding of the smart campus advanced predominantly by technically connected devices, applications, and analytics to crest new educational experiences, services, and operational efficiency. The latest "architecture of participation" in smart environments encompasses not just physical infrastructure, but datafied "communication and meanings" (Bunz and Meikle, 2018), which can manifest in digital content, metadata, and social behaviors, including folk or laypersons' perceptions, mental representations, and human–machine interactions (Cheong and Mossberger, 2021). Accordingly, a communication centered approach toward campus IoT highlights everyday interactions and shared meanings as constitutive of smart campus organization. Hyperconnected systems of in-person and mediated communication among multiple university stakeholders, staff, and students are linked to the collection and application of data, which, in turn, construct the norms and routines of university operations. In this sense, the development of smart campuses needs to be understood as involving complex relationships between different human and non-human actors with varying communicative capacities to address and track members of the academic community, while (re)producing the lifeworld of the university through symbolic interaction and understanding of duties, commitments, and allegiances as a part of civil society (Chambers, 2002).

In particular, a critical IoT campus communication perspective here identifies student tensions to be an important pathway for understanding the social dimensions of smart technologies and datafication, including the criticality of incorporating marginalized voices and perspectives in university governance. Dialectical tensions in mediated communication exist when seeming contradictions are interpreted as ordinary, interdependent, and enacted as unifying links of opposing forces (Cheong et al., 2012; Redden and Way, 2017). These dialectics are marked by hyphenation reflecting hybrid conditions, like interactivity-interpassivity, when individuals' increasing access to mediated human connections are challenged with new response expectations and digital distractions (Davis, 2013).

Here, we extend the dialectical approach to IoT communication, previously applied to exploring the intricate tradeoffs between joint opportunities and risks of digital media adoption among young adults. For example, the dependence–independence dialectic was examined in the context of mobile phone use by American college students who texted and called to maintain close friendships while simultaneously experiencing frustrations and guilt over hypercoordination practices (Hall and Baym, 2012). Tensions over social media also involved convenience–privacy and trust–mistrust of digital content, and meaningful–wasted time of "becoming consumed by their platform use" (Masullo et al., 2020). Similarly, Redden and Way (2017) applied a dialectical framework to explicate how American youths negotiated intricate tradeoffs between access and risks in online activities as they improvised with formal media use in their everyday lives.

In view of the mounting debates on data practices in hyperconnected campus life, it is expected that multiple dialectics are operant with student communication with smart campus IoT systems as they are interactants and subjects of data applied to the production of smart campuses and the knowledge it helps to produce. In dialectically oriented research, one of the most consistent themes involve the display–concealment, and performance–privacy tensions with newer media engagement, for instance with Snapchat (Briziarelli, 2019), and digital wearables like fitness trackers (Zimmer et al., 2020). As "the notion of privacy management is predicated on treating privacy and disclosure as dialectical in nature" (Petronio, 2002: 3), students face the issue of how much to share while embedded in the cultural ideology of control over information boundaries. Moreover, as IoT sensors and cameras become embedded on intelligent campus environments, it becomes important to appreciate layered frictions emerging from the dappled realities of hyperconnectivity. While new technological systems are often celebrated with utopic visions, development of ubiquitous computing and by extension, today's IoT environments are "inherently messy" as "uneven infrastructures are encountered and navigated" (Dourish and Bell, 2011: 42). In higher educational settings, while there is no one smart campus model, Kwet and Prinsloo (2020) noted how the rise of a new "data imaginary" legitimizes technological projects, generated by those who have and can speak with data. Accordingly, what it means to be a smart university requires technology integration "based on CCTV cameras, internet monitoring and IoT for centralized analytics, and big data surveillance for the total university experience" (p. 513).

Consequently, there appears to be critical disjuncture between smart campus life driven by strategic plans of university management, and those experienced by staff and students, the latter group often unaware of datafication with smart applications (Vasileva et al., 2018). The dominant vision pushed with efforts by educational technology companies describing how datafication will improve educational experiences with richer correlations, classifications, and predictive models is arguably a "manifestation of tech hegemony to make our computer-driven societies accept the idea of being 'smart'" (Kwet and Prinsloo, 2020: 512). Not unrelated are calls for universities to serve as testbeds to help governments and corporations work out grander visions of smart city developments (Min-Allah and Alrashed, 2020). The coupling of public–private operations amid data use design raises further questions regarding potential tensions perceived by students in IoT campus communication linked to end-to-end trust and security. Indeed, recent studies have pointed out that despite their seeming nonchalance, young adults harbor concerns on how their personal data are archived and recomposed across digital networks and commercial platforms, though their concerns are concurrently laced with a sense of inadequacy and incapacity (Pangrazio and Selwyn, 2019).

In sum, prior literature demonstrates how dialectics may serve as a useful heuristic to understanding student communication practices in campus IoT systems. Seeming contrasts and contradictions in everyday mediated and automated experiences are not simply elided but are set in productive frameworks of understanding. The presence of tensions illuminates recurring perceptions and concerns of emerging media use, as well as serve as a generative means for envisioning synthetic ideas for problem solving, among young adults who can articulate counter-imaginaries of new media adoption (Cheong and Mossberger, 2021; Redden and Way, 2017). Accordingly, we advance two research questions: (a) How do students describe the dialectical tensions they experience with smart digital campus applications? (b) In what ways do students envision new communicative practices that support alternative data imaginaries with smart campus applications?

Method

Given our research foci, the following empirical study draws upon focus group interviews to investigate our research questions. The use of focus groups is an apt methodological response to calls for more grounded research to examine the meanings of datafication from lay persons' experiences and encounters with smart devices (Cheong and Mossberger, 2021; Ytre-Arne and Das, 2021). As we seek to explore the everyday and emerging communicative practices of student IoT users, qualitative group interviews have proved to be well-suited to comprehending dialectical tensions experienced with new media use among young adults (Masullo et al., 2020; Redden and Way, 2017).

In this study, we interviewed undergraduate students in nine focus groups in a large public American university, recognized among the "most innovative" universities by U.S. News and World Report. This context is well-suited for the purposes of this study as the college is involved in multiple smart campus initiatives including its campus mobile app (with more than 100,000 downloads), sensor-equipped sites, emergency networked systems, and smart lighting across campuses. Smart campus IoT pilot projects being deployed at the time of project initiation included the adoption of a smart speaker by students in a new residential hall, and a study of an introductory course asking students to opt in to track their location using a virtual beacon when they enter the classroom. Under the leadership of its technology office, the university regularly holds "smart campus events" and has partnered with technology and telecommunications corporations to implement 5G internet connectivity and voice-activated services. For example, the latest smart developments reported in 2022 included collaboration to extend wireless Internet connection for smart devices on campus and blue light poles fitted with smart environmental sensors connected across IoT. As claimed by leadership in news stories, IoT innovation is celebrated as a laboratory for "smart solutions" to "scale the use of smart devices effectively and efficiently" for the university and beyond. And like in several other large universities, the push to implement the latest IoT has been debated, echoing concerns expressed in local news about opaque notice and consent processes, as well as device efficacy and privacy concerns including IoT managed by university offices that mine data from student smart ID cards with neither their knowledge (e.g. Harwell, 2019; Jess, 2018) nor a straightforward process of accessing data collected (Johnson, 2019). Students in a residential hall, for example, were mandated to sign a lengthy waiver for Echo dots given, leading some to express negative feedback on the notice and consent process, as well as efficacy of the device and privacy concerns (Thomason, 2017). Hence, with the heightened interest and growing embeddedness of IoT on campus, the setting of this study provided a natural site for meaning-making of situated activities (Given, 2008) where students interact and reside.

After institutional review board approval was secured, interviewees were recruited via newsletters and emails to students on campus and in various dormitories. Fifty-four undergraduates in nine focus groups participated in the study, and recruitment stopped after the group discussions reached saturation when incoming data produced little new information and after a minimum of 3–5 groups that provided thick and rich data (Krueger and Casey, 2000). According to participants who self-reported their gender (83% of the sample), 26 identified as female, 18 as male, and one as non-binary. Different backgrounds were observed among discussants who disclosed their academic major, with the respective numbers represented in various fields: computing and mathematics (10), engineering (9), life sciences (7), business (6), social sciences (5), fine arts (2), and education (1). Participants on average noted that they owned or operated approximately four connected devices, including smart phones, wearables, tablets, and smart home/dormitory devices.

The focus groups were conducted in-person, in conference rooms facilitated by two trained members of the research team, in the Spring of 2020. Participants were offered a US$10 honorarium, and the interviews averaged 60 min. Sessions began with participants introducing themselves, their backgrounds and use of smart technologies, followed by a semi-structured interview route of open-ended conversational questions (Krueger and Casey, 2000) including subjects' perceptions of IoT, reactions to various types of tracking and monitoring, and preferred communication practices and alternative imaginaries within an IoT campus environment. In accordance with best practices for focus group interviews, questions were sequenced (Krueger and Casey, 2000) so conversations flowed from general (e.g. do you think public and educational institutions have the right to collect data about you?) to more specific (e.g. if you could construct a new way in which users could protect their data, and give their consent to mobile app operations, how would you do so?) and to imagination questions (e.g. what is the future of the IoT going to look like for you? How do you think that smart devices and sensors are going to influence your future?).

Using a professional research service, all interviews were transcribed in full (200 pages) for thematic analyses as well as the use of verbatim quotations for reporting the research. They were then subjected to a constant comparative methodology, looking for thematic commonalities in the data, involving a grounded theory approach appropriate for the exploratory analyzes of emerging phenomenon (Charmez, 2006). Line-by-line analyses were used to generate initial codes and suggest relations among them, and then used for iterative review to evaluate the usefulness of developed codes (Strauss and Corbin, 1998), and to refine them into categories using a consensus process to assure the quality and verification of the interpretations presented (Lindlof and Taylor, 2002). Such categorization, driven by our conceptual questions, also ensured that quotations selected to represent students' viewpoints in the paper reflect convergence and consistency of opinions voiced (Lindlof and Taylor, 2002). To protect the anonymity of the discussants, personal names and identifiers are not mentioned but indicated with U(respondent number), gender, and area of study/major.

Results

Experiences of dialectical tensions

Regarding research question one, student interviewees expressed multiple dialectical tensions amid contending forces and interests on their smart campus, which are discussed below as (a) convenience–annoyance, (b) integration–independence, and c) safety–insecurity.

Convenience–annoyance. The first dialectic referred to as convenience–annoyance is evaluative of their IoT interactions as students attach valuable expectations to their university app experience, to augment their campus life while also experiencing uncertainty and frustrations. A third of discussants highlighted positive affordances of campus linked IoT enabled interactions on their smartphones, reflecting the dominant cultural ideology that promote smart technologies as facilitating the personalization of content tailored to individual student needs (Bonderud, 2019).

Accordingly, students highlighted "convenience" as a key relational experience as they installed the campus app to purchase sporting event tickets, check their meal plan balances, navigate classes, locate classrooms, and connect with their course-mates. And yet students also mentioned the troubling frustrations they experienced alongside their use of customized features. The comments below reflect vexations that multiple interviewees shared:

> Sometimes I'll use it to check my meal balance… And then the beginning of the semester I'll…where it says, oh where your building is? And I'll try to do navigate. Sometimes it works, sometimes it doesn't. So, it gets kind of annoying. (U21, female, sustainability major)

> I do like it because obviously it shows me locations of all of my classes …. I guess the unfortunate thing is it doesn't actually say who your professors are, or what time the classes end for each if your classes in your schedule…So, it's a few more steps that could easily just be put on it. (U47, female, engineering management)

Thus, while relying upon campus technologies that appear to be sharing timely and beneficial information, students also shared that they experienced "buggy" user constraints and sub-optimal user interfaces that marred routine interactions, in terms of longer than expected load times. Feedback on their app use experiences included, "its clunky," "hard to navigate," "spotty," and "it doesn't make sense sometimes." For 11 discussants, these tension-filled experiences served to catalyze their periodic digital disengagement, where they "installed it to attend university athletic events and then [u]ninstalled" and "barely use it, once or twice a semester." In this way, quotidian perceptions of smart campus IoT reflect convenient access as well as communicative breakdowns, which poses dynamic and ongoing negotiations of student data practices as they navigate salient needs and disruptions of the moment.

Integration–independence. The second dialectic stems from relational struggles of connection and autonomy as IoT is nearly irremovably woven into datafied campus systems and spaces. Most interviewees generally voiced acceptance of university data collection through IoT integration as a part of their modus operandi. Yet, while some expressed trust in their institution's data tracking and protection practices, over one half of the discussants noted limitations of app consent and IoT operations that do not fully support their data disclosure choices.

Specifically, it was observed how the integration of IoT into everyday campus life brought "attendant struggles of co-dependency" (Baxter, 2009). As students negotiate closer relationships with smart technologies, they construct a meaning of closeness that struggles with the tensions of individual autonomy and interdependent ties, which have been observed with earlier mobile communication (Hall and Baym, 2012). Here, respondents shared how they perceived membership in their institution as bringing about obligations for data sharing, in the context of their disclosures from the college admission process and current enrollment setup.

For example, the following responses highlight how three students understand their institution's data for facilitating tight connectivity and accept helpful intervention:

> [the university] needs your data…If you're a student and you go here, they need to know like your name…your social security number, all that stuff just to verify you're a real person. But I mean certain things that are going on in the background with like the app and everything, it needs to be very clear what they're using that for. (U11, male, biology major).

> I feel they use it to make different simulations of different types of students and assess risk based off that on which students they think might need extra help, which students they think will succeed. (U3, male, political science major)

> I think [location data] could be very useful…. If we know which routines students are making… which are the more congested areas that it might help with future urban planning when it comes to streets and sidewalks, bikes zones or walk-only zones. (U2, male, information systems major)

Another female student majoring in math explained how she understood institutional "access" to a centralized hub of data linked to students' records, like health and fitness, grades and medical status are "all connected to help" students.

Apparently undergirding students' understanding of datafication and its compatibility with their informational needs is trust (Waldman, 2018), in this case, a sense of institutional trust in a non-profit educational setting. A fifth of the respondents expressed how they perceived the significance of "nonprofits like academic are more trusted because they wouldn't monetarily gain from your data." As one student said, "I feel like I trust the [university] a lot more than something like Google or Facebook. Just because it is a public institution. So, it's whereas Google or Facebook interests are in one place, [the university] might be in a more something more aligned with mine" (U43, gender and major not reported).

This perception of educational unit trust appears to be extended to the notice and consent procedure of the university's app installation. Almost all the students did not read the user agreement and some attributed it directly to their belief in the university's governance and operational practices:

> That's just how it is. I also think that it's [the university]… They already have [my data]. Yeah, so like all of my applications for the college have all of the information that is on my phone essentially. So, okay. (U13, female, music major)

> I didn't have too much concern with it because… it asked me if [the university] could release information to [MyCampus] app and I know [the university] is very secure about what they release and what they don't. So, it just left me feel safe linking [the university] app with a [university] affiliated page. (U6, male, business major)

At the same time, students mentioned about the "feeling like there's not really a choice" in the data notice and consent protocol for their campus app, as one female engineering student said, "If you're going to use the app, you're going to use it, you know, so you can't use it without signing this agreement. So, like what are you going to do?" Acknowledging this lack of user agency, students raised issue that not only did they have no choice but to accept the terms if they were to download the app, they also had no choice but to download the app if they wanted to participate in certain university activities. For example, a student explained how the epistemic gap in the seemingly opaque smart interfaces is associated with her ambivalence with the campus connections fostered by IoT:

> Is what exactly? Is that like I really have no idea what's in them. So, you kind of have more of a trust and look props. I don't really know…Like it's just like, Oh I want to use the apps. But now I'm feeling like maybe I should have read [the consent]. (U30, female, math major)

While no specific university public–private partnerships were raised, apparent tensions of integration–independence associated with third party access to university data were voiced, for example by two students who expressed their "love hate" relationship with datafication since "they already have data on me since I became a student" so the [university] has "a right to my data" but "doesn't have the right to give away my data."

Safety–insecurity. The third dialectic highlights students' concerns for IoT that are ostensibly promoted for their safety but paradoxically presents new security risks that this newer suite of technologies has in part helped to usher. This tension primarily unveils conflicting ideologies on what it means to be communicatively open and secure within the IoT ecosystem. Discussants value data sharing to a certain extent but also expressed awareness of the risks of data leakage and misappropriation.

Specifically, students shared that they were urged to "download the campus created app," promoted as helping to enhance[s] one's personal safety across [campuses] by placing more reporting power in the palm of one's hand [campus hyperlink]. Students understood that the app affords them the ability to connect with campus police with tips and emergency calls, request safety escort services, and enable location tracking for services, which are closely linked to augmenting their sense of safety. For example, one said

> I have my location on for my parents…then very few friends here just so they know if I'm somewhere. So, they can check up on the place if I'm not answering. (U22, female, finance major)

In addition, IoT supported campus video monitoring is understood by some as a safeguard, "in the case of security, you need to have security cameras around campus," "for the benefit of the greater good." The capacity for surveillance supported by IoT was also recognized as a safety feature; for example, a student said

> If there was a crime or violence or some massacre happens. Obviously, if it was right here at our school and local, I would want that to be able to try and catch who did it. (U14, female, engineering major)

At the same time, students discussed the joint risks that accompanied the use of the campus app and campus-wide intelligent camera and video monitoring systems. In particular, a third of students debated on their use of the location tracking service and the "balance of security" with campus collection and storage. As there is "certain routine [one] goes through….going to classes and everything," students "frequent a certain amount of areas" so there is daily movement pattern data recorded but this means living dialectically with the risks of IoT communication as one student said

> [E]very single [campus] tour, they're like [campus safety app] is so cool because you can tell people, I'm going from Point A to Point B and you don't have to be at [campus] to do it. And the reasoning behind it sounds really good. If you're going from Point A to Point B, you're letting your friends know you're safe. At the same time, that's still an app that's keeping track of your location. (U28, male, business major)

In line with this view, students raised dark possibilities of potential data abuse, theft, and loss with ambient IoT surveillance. Various discussants mentioned striking scenarios that were perceived to endanger them if data is "being unintentionally access by people who might want to murder, hurt you…" or in occasions where IOT serves as "another gateway for prejudiced people," where the university may be "strong armed by the government" to give up their data, with a risk of "deporting people." Three students explained

> Institutional overreach. So, sort of say you're doing something very minor that the university disagrees with and they now have a facial recognition camera identifying you as the

> person that is doing this minor thing. They can do whatever they want to about that, like you could be blackmailed. (U15, male, engineering major)

> If you're hanging out with your friends and you say something that's against [the university] and they have the audio recording. It's very possible that they could lower some internal score and either they won't give you a scholarship funding or you'll be less likely to be selected for programs. (U19, male, computational math)

> I don't hate [university]. I don't think that they purposely are going to do anything but we've seen with Facebook for example, that information can be hacked and the internet isn't perfect. (U50, female, engineering major)

Correspondingly, together with increased tracking are heightened risks of data misuse and manipulation, which has transpired in a past campus incident where a classmate's photograph was doctored thereby affecting his reputation, as one student (U52, female, engineering major) recalled. Thus, this dialectical tension in what it means to be safe and secure within a smart campus is inflected with a variety of specific scenarios, depending on how students perceive their data is stored, appropriated and shared.

New communication practices and alternative data imaginaries

Regarding research question two, respondents voiced various communicative practices that constitute alternative imaginaries and governance with IoT applications, which are enacted through both new and more established forms of interaction, with (a) app and consent interfaces, (b) older analog and electronic media, and (c) traditional authorities.

Interface and platform redesign

Half of the respondents highlighted ways that the present platform architecture of their campus app could be re-designed with new communiques to better reflect their interests and concerns about datafication. The top feedback centered on "better control" over their data and ways in which interface communication could provide them with "clearer information." One-third of the students expressed that they would like the initial consent procedure to be simpler yet more informative; with less legal jargon and phrased in a language that is more concise and accessible to them, for example, using "bullet points" to highlight key information like "how long is it [data] being kept for," "the assurance to know that it is actually being deleted," and where data is shared and "exactly who[m] it's being shared with."

Referencing their experience with the notice and consent procedures in commercial apps and smartphone platforms, students noted that the [mycampus] app experience should be "more simple and transparent," with "clear disclaimers" on "why my location is being used," and the ways that their app data is shared with other entities and if the university is not selling their data, they have to "delete it" after a certain amount of time.

Twenty-eight students also pointed out that "opt in and opt out messages" should be clearly communicated regarding their location data, preferably constructed as a "system of progressive permissions instead of like a default" allowing the campus app constant location tracking access. Specifically, four discussants shared that they would appreciate "upfront and honest" in-app communications, including prompts and notifications to remind them "to check on their privacy settings" and what "the app's taking from them, giving to them" with "just one easy click."

Connection with older analog and electronic media

Related to smart campus vision sensors and emergency networked systems, about a quarter of the discussants requested for more specific announcements, including the incorporation of older media that signal the presence of these sensors amid their miniaturization and embeddedness. According to the students, it is important that they are informed of "some kind of detailing of what they're tracking….because while the cameras are a system that [university] has complete access to…I don't think about someone watching them." Specifically, three students requested for physical signage to mark these sensors as "they just pop up out of nowhere" and particularly questioned if data captured by environmental sensors are being paired with facial recognition database with other tools "that are not that accurate at all" or if used to "implicate people in crimes." Two respondents asked for "a map identifying where all they are, what the screen shows where like if they are collecting information" and "signs…I think every camera should have like a sign that says this is a camera."

Other forms of older mediated communication were also brought up as being potentially helpful for students to understand smart campus monitoring and oversight. Two thirds majority of the discussants addressed the need for a "centralized location" or a separate web page on the university website "where it has a list of all the data" that is being collected from students, or a "separate disclaimer page" about what sorts of "tracking they [university] are doing." Eight students also suggested the production and dissemination of short, impactful educational videos in the format of the "flight attendant-like safety video" and "email blasts" from school deans and administrators telling them to pay attention to IoT innovations indicating "this is happening, this is kind of major," to signal the significance to them. Another respondent shared that different forms and requirements of digitalized engagement should be presented to students in traditional and quotidian ways, for instance, in their course syllabuses, alongside the student code of conduct and other academic policies. Students also debated on the utility of obtaining visual data access or immediate video playbacks on IoT devices like smart emergency blue light posts. There was no clear consensus if they would like to review the seemingly voluminous "boring" or "repeated" video footage, which might be "creepy" and "awkward" to replay.

Instruction from and interaction with traditional authorities

Notably, within the context of the increasingly mediatized university, interpersonal and face-to-face connections within traditional classroom or group settings were mentioned as significant and prized by some discussants. Twelve students voiced their desire for focused pedagogy related to privacy and data developments in their smart campus environment, for instance, in introductory, general education classes, or "simple workshops offered at [the university]." For example, one said, "I wish we'd be educated about the privacy and stuff in school, even in our 101 classes be educated about it because honestly, I feel a lot of people, myself included don't know about this."

Another discussant who mentioned the importance of in-person instruction said, "[t]own halls with students and then if they, students wanted the option to get rid of some data that [the university] collected, they should have an easy process to do that." In addition, a dozen students stressed the importance of known interpersonal connections to help support their comprehension of datafied and automated practices on campus, for example, one said, "I'd like something that was a little bit more human…to talk to someone." Another student said, "same thing with security. It's not so much an issue until it becomes a problem. And if there was a problem I want to be able to talk to someone…and have somebody actually care to do something."

Discussion

In this contribution, we critically examined the communicative tensions experienced in smart campus operations and governance, documenting student perspectives that have been marginalized in dominant discourse premised on convenience, intuitive integration, and safety facilitated by big data and IoT. Dialectical tensions discussed here underscore historical "messy realities" of ubiquitous computing (Dourish and Bell, 2011) but are updated here to highlight concurrent opportunities and risks that are ironically ushered in with new "smart" technologies and datafication. There are at least three aspects of our findings that inform smart campus developments and governance that we provide additional reflections here: (a) the increasing complexity of student privacy concerns, (b) data normalization and coercion on university campuses, and (c) the changing nature of digital divides and digital inequalities. Taken together, the concluding discussion points to social implications of data governance and future areas of research as critical understanding of datafication catches up with the welter of budding smart innovations.

First, our study findings document and illustrate how intricate privacy concerns which lie at the core of communicative tensions are significant factors in higher educational data engagement, a part of social data governance that warrant added consideration. While in-person privacy and disclosure have been communicatively treated as dialectical in nature (Petronio, 2002), students interviewed experienced multiple communicative tensions linked to growing privacy concerns with campus IoT, which are related to those experienced with social and wearable media (e.g. Masullo et al., 2020; Zimmer et al., 2020) but are not wholly the same. Specifically, students reported that their informational disclosures are enacted within a non-profit institution that many of them trust (Johnson, 2019), while expressively being unsure of potential data breaches and data sharing practices with other entities, within the larger cultural background of potential data misappropriation and interpretive bias. Notably, the relative lack of clarity regarding data access risks by third parties appeared to be related to concerns regarding surveillance, even a perceived violation of norms within universities as protectors of individual rights and freedoms. It is also significant that findings underscore profound issues of trust and privacy that should be attended to in social data governance, in light of campus data breaches at universities in recent years. Vulnerabilities in campus IoT systems expose personal identifiable information of students, who have expressed frustration because they "trusted the university," yet did not receive clarification of their data exposure nor follow-up support from the university beyond the initial news of data leakage (Chouinard, 2021).

In addition, as highlighted in the dialectics of convenience–annoyance reported in the findings, the very convenience that students reported to enjoy with their campus apps involved communication gaps or breakdowns, and often necessitated their data management or input. And consequently, because IoT data archival occurs ceaselessly and in the very routines of daily campus living which tend to go unnoticed, this extraction generated deeper privacy concerns about their present, as well as what Ytre-Arne and Das (2021: 14–15) call the "increasingly prospective" uncertain and future oriented datafied communication, in this case, when students apply for scholarship and grant programs or apply for internships and jobs. In these ways, our findings illustrate the claims in various commentaries about the paradox of smart systems, related to its widespread accessibility and user-intuitiveness yet relative invisibility and elevated risks (van Deursen and Mossberger, 2018) which belie the profound conundrums and emerging frictions accompanying its uptake.

As such, the second dialectical tension of integration-independence identified in the findings underscore present and potential thickening binds that students are embedded, as universities adopt networked technologies while serving as a living laboratory and product test bed for smart cities (Kwet and Prinsloo, 2020). As discussed in this paper, the relationship between a student and their university in terms of datafication is growing in complexity, encircling education, housing, extracurriculars, dining and employment, as well as in recent years, added details on location, movement, health, and biometrics. Accordingly, in terms of policy and governance, smart campus developments raise deeper questions about dataveillance, specifically the norms and ethics of cooperative surveillance and data sharing within a trusted system that perceptibly "needs" students' data to survive, yet presents them with "no choice" when scarce consent protocols and alternative platforms are available for students to sign up, in order to remain engaged with campus events without being tracked.

Second and related to the above, various practices associated with smart campus organizing appeared to be problematic to students who articulated feeling a loss of communicative autonomy (Chambers, 2002), even a sense of "coerced digital participation" (Barassi, 2019) amid hyperconnectivity. It is notable that in this context as well as in other campus settings, students report their joint frustrations and relative lack of power to provide critical feedback on the rollout of campus apps (Bradford, 2018), inability to obtain prompt clarification or request the data being obtained from them (Johnson, 2019), and the inability to opt out of campus wide monitoring systems (Mangan, 2021). This state of affairs with the development of smart campuses has wide-ranging implications for datafied normalization, beyond the university sporting arena where the phenomenon was first described (Yang and Cole, 2022). Algorithmic systems, their practices, and values influence broader standards and social relations (Grosman and Reigeluth, 2019), to students' everyday lived experiences where IoT is bound up in rendering their behaviors archivable and governable.

Specifically, findings in this study illustrate the complex and constrained role of human communicative action as student users navigate and interact within emerging campus IoT systems that normalize university monitoring and control (Yang and Cole, 2022), under conditions that seem less than transparent and equitable. While acknowledging the conveniences and safety benefits supported by newer smart applications, dialectical tensions marked students' relations with campus technologies that are not wholly supportive of their user experiences and desire for the freedom of choice to manage personal informational boundaries. In light of conflicting communicative practices expressed, this elevates the significant concerns regarding how data governance enacted by educational institutions may curb and undermine the civic foundations and pedagogical purposes of tertiary schools. As Stommel (2014) argued on the potential of educational technology to both oppress and liberate, "…[r]eal education is not possible without agency…if we don't feel like the welfare of our data and privacy is in our own hands, we are less likely to feel like full agents in our learning." Taking into consideration the historic value of American universities as guardians of civil liberties and democracy (Tierney, 2021), the presentation here related to data normalization opens up broader considerations of the rights, hopes, and aspirations of student users and their communicative autonomy, particularly the need to allow students to make critical decisions about what happens to their data.

Although data governance by school leadership is not novel, critical attention to expanded communicative practices linked to the regulation of campus networked applications and sensors is lagging. As Shorey and Howard (2016) observed in their critical review of algorithms, automation, and big data, because few projects integrate information ethics, there are adverse effects on individual autonomy and social equity. Hence, the oversight and continuous review of data collection and the day-to-day extraction processes enabled by IoT technologies need to be prioritized by university leadership. Indeed, the second part of the results speaks to the significance of cultivating a multivocal dialogue in the ongoing development of the smart campus, as students articulate a diversity of imaginaries that prioritize their data needs and protection. Cognizant that shared governance practices within universities are fracturing in light of "the neoliberal environment that prizes the speed that decisions can be made rather than the process of deliberation about issues" (Tierney, 2021: 17), informed discussions on strategic plans about newer IoT systems should consider diverse interests and entities, beyond the province of senior administration and governing boards. Students' input should be incorporated from the start through co-design on matters of data security that transfer to new and emerging IoT environments, and not merely reacted to, or listened to after IoT rollout or public reckonings recognized as "techlash." At the least, educational providers should commit to collaboratively conceived principles that support students (Morris and Stommel, 2013), and proffer lucid accounts of how student data collected will be used and made available to others, and how their connections support their institutions' financial health. Therefore, in light of multiple dialectical tensions etched onto students' daily digital interactions, the fulfillment of smart campus developments needs to reconcile institutional growth with students' present and emerging queries and concerns regarding their physical privacy and data security.

Third, findings here have significant implications for understanding "second-level" and "third-level" digital divides, after primary internet access has been bridged (Scheerder et al., 2017) on many college campuses. A key argument in the digital divide literature is that newer technologies may exacerbate existing social inequities, since individuals' capacities and stock of investments to translate online connectivity to favorable outcomes differ (Lutz, 2019). Here, as students have voiced their needs for more classes, workshops and public forums on IoT data practices, this raises the issue of how participation on smart environments may require new digital literacies and skills, to empower student interactants to become more aware and actively engaged. Second-level digital inequalities involving Internet skills and uses can be ameliorated with new curriculum (or in the words of students', "workshops" or content embedded in "general education" courses) to provide flexible and accessible instruction, beyond mechanical knowledge of IoT to lessons on critical digital literacies, data uses, and reflexivity (Pangrazio and Selwyn, 2019), tailored to reflect contemporary IoT innovations.

Furthermore, framing IoT communication tensions dialectically provides a useful heuristic to shed more light on potential harms and opportunities afforded by intensifying networked campus connectivity. Recent research attention has pressed for investigations into emerging third-level digital divides, which refer to differences in gains from Internet use including benefits for personal productivity and well-being, and longer-term outcomes like a sense of social belongingness (Lutz, 2019; Van Deursen and Helsper, 2015). In particular, findings here further underscore how research should not only study the profits but also the harms of digital connectivity, which appear to be endemic in IoT connectivity as risks and gains are not either/or but are intertwined and perceptibly co-present (Lutz, 2019). Viewed from the lens of the dialectics in IoT campus communication, the discussion here moors us conceptually to the dualistic nature of competing demands as students felt like they were disproportionately monitored or concerned about being left out or disadvantaged by their digital traces. In turn, these stresses and concerns about surveillance have ramifications on their college life, including their sense of well-being and belonging to their campus community.

Limitations and future research

The limitations of this paper are acknowledged, alongside recommendations for future research. First, this paper drew from a purposive sampling of college students from multiple disciplines, including the natural sciences and a smaller proportion from the social sciences and humanities. While generalizability of the sample was not sought in this exploratory study in a U.S. higher education context, future studies could examine a wider subject pool and investigate the expanding range of sensing technologies that animate data normalization practices among other constituents of the smart campus, including academic and non-academic staff. Furthermore, the challenges of coerced digital participation experienced within campus IoT ecosystems could be further studied in future comparative research in international settings, to advance a more comprehensive picture of enduring tensions and the cross-cultural variants.

Second, while the broader backdrop of IoT surveillance on university platforms is recognized together with potential data breaches and long-term constraints on civil liberties, it was beyond the scope of this paper to delve comprehensively into specific governance policies and detailed claims of the university IoT infrastructure and functionalities. In future papers, extended analysis on the explicit and implicit claims of universities' IoT visions, systems and capacities would provide additional contextual understanding of different stakeholders' perceptions and interactions, experienced with varying levels of awareness of university public–private IoT partnerships. Future research could also investigate the impact of macro conditions like how the health and safety concerns of the global health pandemic, which at the time of writing is experiencing a resurgence of alarm, will affect the establishment of new campus data architecture and behavioral mandates overtime.

Last but not least, while this study was focused on qualitative inquiry, future multimethod studies can investigate the antecedents and consequences of third-level digital divides, to identify differentiated outcomes of students' smart campus application adoptions, including how different constituents may reorient tensions to new sources of creativity and dialogue. An intersectional research approach also could be applied to quantitative and mixed method studies to identifying and helping traditionally disadvantaged student groups, who may experience the most tensions and vulnerabilities associated with IoT rollouts. Furthermore, as students discussed the importance of connecting with traditional authorities and in face-to-face settings regarding their data concerns, findings here highlight the need for future research on the role of interpersonal and human communication in moderating digital divides, amidst IoT encounters which may devalue in-person interactions. Subsequently, future research should attend to how diverse social support staff like program coordinators, peer mentors, and resident advisors in college dorms may play an outsized role to help students meaningfully navigate smart interfaces or customize app settings, to facilitate less stressful or invasive campus experiences. In sum, visions of the smart campus and by extension, smart environments are held up here for scrutiny not as frictionless abstractions, but as cardinal sites for understanding and thriving in power asymmetries, human communication and imaginaries in times of hyperconnectivity.

Acknowledgments

We would like to express our appreciation to Stephanie Gerhart who helped with the project's data collection.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID iDs

Pauline Hope Cheong https://orcid.org/0000-0002-6971-9115
Pratik Nyaupane https://orcid.org/0000-0001-5558-7599

References

Anderson J and Rainie L (2012) Millennials will benefit and suffer due to their hyperconnected lives. Report, February. Pew Research Center, Washington, D.C.

Barassi V (2019) Datafied citizens in the age of coerced digital participation. *Sociological Research Online* 24(3): 414–429. DOI: 10.1177/1360780419857734.

Baxter LA (2009) Dialectical processes. In: Reis HT and Sprecher S (eds) *Encyclopedia of Human Relationships*. Thousand Oaks: Sage, 418–420.

Beer D (2019) *The Data Gaze*. London: Sage.

Bonderud D (2019) How Arizona State University built a smart campus. Available at: https://edtechmagazine.com/higher/article/2019/12/how-arizona-state-university-built-smart-campus-perfcon (accessed 20 March 2020).

Bradford A (2018) UC Berkeley to launch new campuswide app despite concerns from ASUC. Available at: https://www.dailycal.org/2018/03/16/uc-berkeley-launch-new-campuswide-app-despite-concerns-asuc/ (accessed 4 April 2020).

Briziarelli M (2019) Snapchat's dialectics of socialization: Revisiting the theory of the spectacle for a critical political economy of social media. *Communication, Culture & Critique* 12(4): 590–609. DOI: 10.1093/ccc/tcz029.

Bunz M and Meikle G (2018) *The Internet of Things*. Cambridge: Polity Press.

Chambers S (2002) A critical theory of civil society. In: Chambers S and Kymlicka W (eds) *Alternative conceptions of civil society*. Princeton, NJ: Princeton University Press, 90–110.

Charmez K (2006) *Constructing Grounded Theory: A Practical Guide Through Qualitative Analysis*. London: Sage.

Cheong PH and Mossberger K (2021) Voicing the future: Folk epistemic understandings of smart and datafied lives. In: Katz J, Floyd J and Schiepers K (eds) *Perceiving the Future Through new Communication Technologies. Robots, AI & Everyday Life*. Switzerland: Palgrave Macmillan, 195–208.

Cheong PH, Martin JN and Macfadyen L (2012) Mediated intercultural communication matters: Understanding new media, dialectics and social change. In: Cheong PH, Martin JN and Macfadyen L (eds) *New Media and Intercultural Communication: Identity, Community and Politics*. New York: Peter Lang, 1–20.

Chouinard K (2021) 'We trusted the university': Students affected by SU data breach express frustration. Available at: https://www.dailyorange.com/2021/09/students-syracuse-university-data-breach-frustration/ (accessed 30 December 2021).

Clark BR (1963) The "cooling-out" function in higher education. In: Smelser NJ and Smelser WT (eds) *Personality and Social Systems*. New York: John Wiley & Sons, pp. 229–237. https://doi.org/10.1177/0725513613500268

Davis M (2013) Hurried lives: Dialectics of time and technology in liquid modernity. *Thesis Eleven* 118(1): 7–18.

Dourish P and Bell G (2011) *Divining a Digital Future: Mess and Mythology in Ubiquitous Computing*. Cambridge: MIT Press.

Given LM (2008) Research setting. In: Given LM (ed) *The Sage Encyclopedia of Qualitative Research Methods*. Thousand Oaks: Sage, 787–788.

Grosman J and Reigeluth T (2019) Perspectives on algorithmic normativities: Engineers, objects, activities. *Big Data & Society* 6(2): 1–12. DOI: 10.1177/2053951719858742.

Hall JA and Baym NK (2012) Calling and texting (too much): Mobile maintenance expectations, (over) dependence, entrapment, and friendship satisfaction. *New Media & Society* 14(2): 316–331. DOI: 10.1177/1461444811415047.

Harwell D (2019) Colleges are turning students' phones into surveillance machines, tracking the locations of hundreds of thousands. Available at: https://www.washingtonpostcom/technology/2019/12/24/colleges-are-turning-students-phones-into-surveillance-machines-tracking-locations-hundreds-thousands/ (accessed 25 February 2020).

Herold B (2019) Schools are deploying massive digital surveillance systems. The results are alarming. Available at: https://www.edweek.org/leadership/schools-are-deploying-massive-digital-surveillance-systems-the-results-are-alarming/2019/05 (accessed 22 January 2020).

Hobohm T (2019) Alexa, why are you here? Available at: https://utdmercury.com/alexa-where-are-you-here/ (accessed 21 January 2020).

Jess S (2018) Student ID Card research raises privacy concerns. Available at: https://news.azpm.org/p/news-articles/2018/4/3/126752-catcard-research-raises-privacy-concerns/ (accessed 2 February 2019).

Jessop B (2018) On academic capitalism. *Critical Policy Studies* 12(1): 104–109. DOI: 10.1080/19460171.2017.1403342.

Johnson S (2019) Inside a student's hunt for his own learning data. Available at: https://www.edsurge.com/news/2019-05-28-inside-a-student-s-hunt-for-his-own-learning-data (accessed 9 September 2020).

Krueger RA and Casey MA (2000) *Focus Groups, a Practical Guide for Applied Research*, 5th ed. Thousand Oaks: Sage.

Kwet M and Prinsloo P (2020) The 'smart' classroom: A new frontier in the age of the smart university. *Teaching in Higher Education* 25(4): 510–526. DOI: 10.1080/13562517.2020.1734922.

Lindlof T and Taylor B (2002) *Qualitative Communication Research Methods*. Thousand Oaks: Sage.

Lutz C (2019) Digital inequalities in the age of artificial intelligence and big data. *Human Behavior and Emerging Technologies* 1(2): 141–148. Available at: https://onlinelibrary.wiley.com/doi/epdf/10.1002/hbe2.140.

Mangan K (2021) The surveilled student. Available at: https://www.chronicle.com/article/the-surveilled-student (accessed 16 February 2021).

Masullo GM, Riedl MJ and Tenenboim O (2020) Dialectics of complexity: A five-country examination of lived experiences on social media. *Social Media + Society* 6(4): 1–11. DOI: 10.1177/2056305120965152.

Min-Allah N and Alrashed S (2020) Smart campus—A sketch. *Sustainable Cities and Society* 59: 1–15. https://doi.org/10.1016/j.scs.2020.102231.

Morris SM and Stommel J (2013) A bill of rights and principles for learning in the digital age. Available at: https://hybridpedagogy.org/bill-rights-principles-learning-digital-age/ (accessed 8 December 2021).

Pangrazio L and Selwyn N (2019) 'Personal data literacies': A critical literacies approach to enhancing understandings of personal digital data. *New Media & Society* 21(2): 419–437.

Petronio S (2002) *Boundaries of Privacy: Dialectics of Disclosure*. Albany: SUNY Press.

Prandi C, Monti L, Ceccarini C, et al. (2020) Smart campus: Fostering the community awareness through an intelligent environment. *Mobile Networks and Applications* 25(3): 945–952. DOI: 10.1007/s11036-019-01238-2.

Rawolle S and Lingard B (2014) Mediatization and education: A sociological account. In: Lundby K (ed.) *Mediatization of Communication*. Berlin: De Gruyter Mouton, 595–616.

Redden SM and Way AK (2017) 'Adults don't understand': Exploring how teens use dialectical frameworks to navigate webs of tensions in online life. *Journal of Applied Communication Research* 45(1): 21–41. DOI: 10.1080/00909882.2016.1248465.

Scheerder A, Van Deursen AJM and Van Dijk JAGM (2017) Determinants of internet skills, uses and outcomes. A systematic review of the second- and third-level digital divide. *Telematics and Informatics* 34(8): 1607–1624. DOI: 10.1016/j.tele.2017.07.007.

Shorey S and Howard PN (2016) Automation, algorithms, and politics| automation, big data and politics: A research review. *International Journal of Communication* 10(24): 5032–5055. Available at: https://ijoc.org/index.php/ijoc/article/view/6233/0.

Shwayder M (2020) As college resumes, students protest against invasive proctoring apps. Available at: https://www.digitaltrends.com/news/cuny-brooklyn-baruch-college-proctoring-apps-student-surveillance-proctorio/ (accessed 5 June 2021).

Stommel J (2014) Trust, agency, and connected learning. Available at: https://hybridpedagogy.org/trust-agency-connected-learning/ (accessed 15 December 2021).

Strauss A and Corbin J (1988) *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. Thousand Oaks: Sage Publications.

Tate E (2018) 2,300 echo dots put Alexa skills in every Saint Louis University dorm. *Edscoop*, 13 August. Available at: https://edscoop.com/saint-louis-university-amazon-alexa-echo-dot/ (accessed 10 September 2018).

Tettlema (2020) ASU and Sprint launch emergency call box project to improve campus safety. Available at: https://uto.asu.edu/asu-and-sprint-launch-emergency-call-box-project-improve-campus-safety (accessed 5 January 2021).

Thomason A (2017) ASU Tooker house residents disappointed with donated Amazon Echo dots. Available at: https://mylocalnews.us/arizona/asu-tooker-house-residents-disappointed-with-donated-amazon-echo-dots/ (accessed 5 January 2018).

Tierney WG (2021) *Higher Education for Democracy: The Role of the University in Civil Society*. Albany: SUNY Press.

Van Deursen AJ and Helsper EJ (2015) The third-level digital divide: Who benefits most from being online? *Communication and Information Technologies Annual* 10(2): 29–52. DOI: 10.1108/S2050-206020150000010002.

Van Deursen AJ and Mossberger K (2018) Anything for anyone? A new digital divide in internet-of-things skills. *Policy and Internet* 10(2): 122–140. DOI: 10.1002/poi3.171.

Van Dijck J (2014) Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology. *Surveillance & Society* 12(2): 197–208. DOI: 10.24908/ss.v12i2.4776.

Vasileva R, Rodrigues L, Hughes N, et al. (2018) What smart campuses can teach us about smart cities: user experiences and open data. *Information* 9(10): 251–264. DOI: 10.3390/info9100251.

Waldman AE (2018) *Privacy as Trust: Information Privacy for an Information age*. Cambridge: Cambridge University Press.

Whittaker Z (2020) Fearing coronavirus, a Michigan college is tracking its students with a flawed app. Available at: https://techcrunch.com/2020/08/19/coronavirus-albion-security-flaws-app/ (accessed 29 December 2020).

Yang C and Cole CL (2020) Smart stadium as a laboratory of innovation: Technology, sport, and datafied normalization of the fans. *Communication & Sport* 10(2): 374–389.

Ytre-Arne B and Das R (2021) Audiences' communicative agency in a datafied age: interpretative, relational and increasingly prospective. *Commnunication Theory*. 31(4): 779–797.

Zimmer M, Kumar P, Vitak J, et al. (2020) 'There's nothing really they can do with this information': Unpacking how users manage privacy boundaries for personal fitness information. *Information, Communication & Society* 23(7): 1020–1037. DOI: 10.1080/1369118X.2018.1543442.

Zuboff S (2019) *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: Public Affairs.