Techné: Research in Philosophy and Technology ISSN: 2691-5928
25:1 (2021): 162–183 DOI: 10.5840/techne2021226135

Big Brother Goes to School: Best Practices for Campus Surveillance Technologies During the COVID-19 Pandemic

Ryan Jenkins, Zachary I. Rentz, and Keith Abney

Abstract: Few sectors are more affected by COVID-19 than higher education. There is growing recognition that reopening the densely populated communities of higher education will require surveillance technologies, but many of these technologies pose threats to the privacy of the very students, faculty, and staff they are meant to protect. The authors have a history of working with our institution's governing bodies to provide ethical guidance on the use of technologies, especially including those with significant implications for privacy. Here, we draw on that experience to provide guidelines for using surveillance technologies to reopen college campuses safely and responsibly, even under the specter of covid. We aim to generalize our recommendations, so they are sensitive to the practical realities and constraints that universities face.

Key words: COVID-19, surveillance, higher education, facial recognition, location tracking, contact tracing

Few sectors are more affected by COVID-19 (hereafter, covid) than higher education. It threatens monumental disruptions to these crucial economic engines for local communities, drivers of the development of knowledge and civics, and a prime source of national prestige. But every crisis is also an opportunity; the question is whether we will take advantage.

Ryan Jenkins, Philosophy Department, California Polytechnic State University, San Luis Obispo, 1 Grand Ave, San Luis Obispo CA 93405; ryjenkin@calpoly.edu.

Zachary I. Rentz, Philosophy Department, California Polytechnic State University, San Luis Obispo, 1 Grand Ave, San Luis Obispo CA 93405; zrentz@calpoly.edu.

Keith Abney, Philosophy Department, California Polytechnic State University, San Luis Obispo, 1 Grand Ave, San Luis Obispo CA 93405; kabney@calpoly.edu.

In this paper, we focus on campus-based institutions of higher learning in the United States of America. We are confident that much of what we say would apply to online-only universities and those abroad. However, our primary experience (from which we derive these recommendations) is with advising universities in America that operate primarily in-person.

There is growing recognition that surveillance technologies could play a role in fully reopening the churning and densely populated communities of higher education. For example, Will Knight (2020) says that a cottage surveillance industry is blossoming, pitching schools and universities on everything from automated contact tracing apps to temperature-reading infrared cameras, AI-enabled cameras for monitoring social distancing or mask-wearing, and location- and health-tracking Bluetooth beacons (Roxby 2020; Miller 2020; Jargon 2020; Heilweil 2020; Burke 2020). Many of these technologies pose threats to the privacy of the very students, faculty, and staff they are meant to protect. These groups are often marginalized in campus decision-making—and those who belong to historically under-represented groups may suffer the compounded effects of multiple marginalizations.

Responding to covid could require collecting new data and synthesizing it with sensitive databases universities already maintain—including healthcare information, student and faculty schedules, live location data, and so on—to track or model the spread.[1] Universities have even considered collecting records of students' financial transactions as a way of reconstructing a history of their whereabouts, for example, knowing that they bought breakfast at one campus dining hall and then visited the bookstore immediately afterward.[2] The prime attraction of using these data is that they can be collected 'unintrusively' (Mittelstadt and Floridi 2016, 305).[3] But synthesizing multiple disparate sources into an enhanced data set like this is itself a potential privacy violation (Calo 2011). Moreover, the use of artificial intelligence for tracking infections and tracing contacts raises its own ethical issues, which have led to a growing literature (for example, IEAI 2020; Floridi 2020; Morley et al. 2020; Tzachor et al. 2020). And situations exactly like this one, i.e. responding to a public health emergency, have been floated before as precisely the kind of situation that might merit bending the traditional rules of data science (Zook et al. 2017, 7–8). The result: universities find themselves in an unenviable, ethically precarious situation.

In this context, ethics concerns the "choices we make at critical junctures . . . that invariably have impact," and requires considering the best reasons we have for acting that balance competing values (Markham 2016) in order to "minimize and manage" the risk of harms (Ballantyne 2018, 2). The authors have a history

of working with our institution's governing bodies to provide ethical guidance on the use of technologies, especially those with significant implications for privacy. Here, we draw on that experience to provide guidelines for using surveillance technologies to reopen college campuses safely and responsibly, even under the specter of covid.[4] Ethical concerns need to be addressed immediately, while technical standards are still taking shape. An ounce of prevention is worth a pound of cure.

1. Our Approach to Privacy

Ethical issues pervade the implementation of surveillance technologies on campus, even when their use is justified by an unquestionable public need. The central concern is privacy—with adjoining concerns about consent, coercion, and the distribution of benefits and burdens, among others. We prefer to view privacy through Helen Nissenbaum's framework of contextual integrity (Nissenbaum 2011, 2004). The most fruitful way of understanding privacy is not to ask which data are *public* and which are *private*, as if privacy were a binary property (Zook et al. 2017; Nissenbaum 2009; Marwick and boyd 2014). Rather, privacy concerns "specific norms and expectations that govern communication among various parties at different times and places" (Lewis-Kraus 2018). Accommodating concerns about privacy requires taking data subjects'[5] reasonable expectations about data flows into account, as well as contextual facts, since there is "no one-size fits all framework" for ethical data collection and management (Ballantyne 2018, 1). Instead universities must negotiate the "competing interests" of their traditional obligations toward their students and faculty and, now, their novel obligations grounded in public health (Ballantyne 2018, 1).

Take, for example, the use of facial recognition technologies on campus. Cameras that can measure temperature have been suggested as part of a surveillance strategy for monitoring the spread of disease, since fevers accompany many cases of covid (CDC 2020a). Concern about facial recognition varies broadly among the public and different applications of facial recognition fall along a spectrum of ethical risk. Hundreds of millions of users are comfortable using facial recognition to unlock their Apple iPhones with "FaceID"—but Americans are usually aghast when learning of China's system of ubiquitous surveillance and are wary of efforts to surveil citizens using facial recognition (Auxer and Rainie 2019).[6]

Offering a nuanced evaluation of the ethical risk of surveillance technologies requires considering several questions:

1. What data are being collected and how sensitive are they?
2. Do users know—or should they reasonably know—that their data are being collected, stored, and used?
3. Who owns and controls the data, and how trustworthy are they? How are data being retained and protected against leaks?
4. Could the data be transferred to third parties—either intentionally as part of "mission creep" or forcibly, e.g. as a result of court order?
5. What is the risk of unintended harm? Is there a potential for abuse by employees, the public, or the government?
6. How do the most vulnerable users stand to be affected?
7. How might bystanders have their personal information collected "incidentally"?

2. Ethical Guidelines for Covid-related Campus Surveillance Strategies

Some caveats are in order first. Note that we are neither epidemiologists nor lawyers. These lessons are meant to illuminate ethical guardrails and guidelines to be balanced against other concerns that confront universities ahead of reopening. Colleges differ widely with regard to their density, the percentage of students living on-campus, whether they are located near a major airport, their class sizes and durations, and other risk factors for communicating covid. We aim to generalize our recommendations, so they are sensitive to the practical realities and constraints that universities face. Finally, many of the guidelines below are synthesized from the literature on the use of Big Data for health research, since much of the debate concerning the collection and reuse of surveillance data has focused there. However, much of those concerns would still apply if, say, "patients" were replaced with "students and staff" throughout.

2.1. Data Collection

1. Abide by data minimization practices: collect and store no more data than is strictly necessary and can be justified by an immediate public safety need.

First of all, collect only necessary data that can be immediately justified by a public safety need. We expect that universities will encounter arguments for collecting as much data as possible: not just health records, or schedules, but faceprints for logging movements, real-time locations from Wi-Fi connections, financial trans-

actions to help establish contacts, and so on. Each of these data sets taken individually is already highly sensitive. Their collection and combination threatens to turn a data lake into a maelstrom of potential privacy violations. The benefits of some of these data sets are speculative or redundant—for example, if students' real-time locations are available from Wi-Fi connections, then students should not *also* be subjected to facial recognition and the collection of financial records for the same apparent purpose. Discharging the obligation of data scientists to "minimize potential harm" begins with collecting as little data as is absolutely necessary (Zook et al. 2017, 1). Those collecting data must be able to "justify why access to particular data is necessary to achieve the research objectives" (Ballantyne 2019, 363). More precisely, universities should consider the *marginal benefit* of collecting, integrating, and analyzing each additional data set, keeping in mind that both the potential benefits and the potential harms could grow exponentially with each new fused data set, making them difficult to calculate and weigh.

Guard against secondary uses of data that go beyond the purpose of the original collection. For example, data about when faculty or staff are on campus, or how much time they spend on campus, could conceivably be consulted for decisions about retention, promotion, and tenure. Data about disease vectors and spread could be used to implicate students in attending parties or other forbidden gatherings. The data protection regime—including policies concerning collection, storage, access, and eventual destruction—must boast a stringency that matches the sensitivity of these data. Angela Ballantyne echoes Nissenbaum when she lists some relevant considerations for data custodians: "To what degree will data subjects' preferences determine how the data is used? . . . Is the data use novel and original or is it likely to be consistent with the expectations of data subjects?" (2018, 2). Elsewhere, she says:

> Innovative uses of health data are typically outside the parameters of the original patient consent, and many were not even foreseeable uses of the data at the point of data collection. Future uses of data may not be consistent with the data subjects' expectations and the purposes for which they originally disclosed their health information. (Ballantyne 2019, 359)

While Ballantyne is above addressing herself to the issue of repurposing health data for novel research, considering the relevance of the quote for our present purposes only underscores the importance of what she says. Data that universities may help themselves to includes a mix of data that were originally given with consent, such as health data; without consent, such as class schedules; and which have

been repurposed from their original context, or which students may not know are being collected at all, such as social media, financial, or location data. Ultimately, whether these data are permissible to use depends on whether their anticipated social benefit can justify their presumed violation of data subjects' consent and reasonable expectations. In all cases, the presumption should be in favor of collecting less data, not more.

2. For data that must be collected, pursue robust methods of anonymization. Appreciate the implications of weakly anonymized data.

Brent Daniel Mittelstadt and Luciano Floridi call anonymization the "minimum requirement necessary to protect data subjects' privacy" (2016, 317). Contact tracing and monitoring should be carried out in a way that is efficacious but anonymous. Inform community members of exposure to the virus while also respecting privacy concerns—and FERPA and HIPAA rights[7]—of those who have tested positive. Decentralized contact tracing technologies, like those promulgated by Apple and Google's joint API, represent an operationalization of this primacy of privacy (Apple, Inc n.d.). All contact tracing apps notify users of when they have been in proximity to someone who has tested positive. Centralized approaches do this by "uploading anonymized data . . . to a remote server where matches are made with other contacts" (Criddle and Kelion 2020). Compare this to the approach championed by Apple and Google, where each participating phone downloads the centralized database in order to perform *its own* analysis and matching, thereby offering greater privacy protections to users and reducing—though not eliminating—concerns (Crocker et al. 2020).

Community members will likely be uneasy about giving up access to location or health information—as around 7 in 10 Americans are unlikely to use a contact tracing app (Gitlin 2020).[8] The mere thought of being tracked, in situations like these, can constitute a harm that must be balanced against any public safety benefits (Calo 2011). Appreciate that the data being collected and stored represent human beings—that "data are people" (Zook et al. 2017, 2)—and that "even seemingly innocuous and anonymized data have produced . . . detrimental impacts" (2017, 2), and the same is true for data collated and released in aggregate (2017, 3). Considering whether to track students off campus is even more troubling, though the data would clearly have value, for example, in revealing who was at a party with someone who later tested positive for covid. It is not clear whether a university could legally collect such data. Ethically, it is clearly harder to justify than restricting surveillance activities to on campus.

We should not rely too heavily on data anonymization techniques post-collection. Despite official assurances, it is notoriously difficult to anonymize large data sets, especially those containing location information (Hern 2019; Schneier 2007; Ballantyne 2018; Ballantyne 2019).[9] Systems for honoring privacy, including robust means of opting out and anonymization, must be in place before any surveillance strategy is implemented.

> 3. Recognize the mission creep that attends the creation of enhanced data sets—most importantly that they can become attractive targets for law enforcement.

Government agencies, including immigration authorities, have an established record of seeking data from any source that might be useful in solving a crime—even when that crime is trivial or the likelihood of benefit is far-fetched.[10] Moreover, a university will often comply with a request from law enforcement rather than risk the cost of a legal battle.

Information about student contacts, schedules, locations, etc., could prove irresistible. So, simply accumulating the data is not a victimless act: it creates an "attractive nuisance" for law enforcement. In technology ethics, this is known as the "*If you build it, they will come*" principle (O'Doherty et al. 2016). These practices may also conflict with commitments made by a university to protect undocumented students or DACA beneficiaries, setting up a legal contest whose outcome would be unclear. Lastly, students' knowledge of the government's potential access to this data could further drive noncompliance.

Matthew Zook et al. (2017, 5) helpfully point out that data that derive from social actions—e.g. those in "highly context-sensitive spaces" (boyd and Crawford 2012)—are likely to be open to multiple meanings, raising the possibility of misinterpretation or wrongful attribution of guilt. There are multiple reasons, for example, why a student might break curfew, and some are entirely justifiable, but this nuance may be lost if the data is shorn from its original context, e.g. in the process of transfer (Andrejevic 2014).[11] Once again, the best way to avoid these entanglements is to minimize data collection and retention.

> 4. Follow best practices for data retention. Robustly secure data against the possibility of leaks or transfer.

Minimize the data that are retained and the length of retention. For example, consider destroying health records that are collected as part of this enhanced data set, e.g. after 15 days or so, when patients are no longer contagious. After this point,

these data no longer serve an immediate public safety need. (Mittelstadt and Floridi call this a "right to data expiry" (2016, 330).) The data could remain in their rightful place, e.g. in the records of the campus health center or local hospital. But they should be purged from any centralized, enhanced or "fused" data set.

The temptation to reuse data beyond its original purpose is "at the heart of Big Data," say Mittelstadt and Floridi (2016, 313), and the heterogeneity of Big Data, combined with the ability of analysis to uncover previously unnoticed patterns, is perhaps its primary attraction. These data would prove attractive both to external threats like hackers and because of the internal temptation to reuse data for secondary purposes that go beyond the original expectations of users. This is in addition to the possibility of accidental disclosures. (Of course, in addition to all of this, universities should be mindful of the legal constraints on data retention and deletion.)

In order to avoid these downstream complications, universities should minimize data collection from the beginning. Articulate and publicize policies around data storage, including the purposes for which it will and will not be used or transferred (if it will be transferred at all.). Under what conditions might these sensitive data leave the possession of the university?

Notice there are good reasons for retaining and transferring data:

> The need to share health information across borders during public health emergencies has been well articulated. Public health sharing during the 2003 outbreak of severe acute respiratory syndrome (SARS) helped control the virus and prevent the disease from becoming established. . . . Now the benefits of sharing more routine public health surveillance data are being recognized. (Ballantyne 2019, 362)

But universities should not take this as a blank check to surveil now and seek justifications later. Consult best practices on health data sharing, such as those promulgated by the World Medical Association's Taipei declaration (World Medical Association 2016) and the World Health Organization (2017). Develop and publicize these guidelines ahead of time, since they are a crucial component of informed consent for those submitting to surveillance. Consider the circumstances under which data might be transferred to local health authorities, for example, and guarantee that this could be done in an anonymized and minimized manner. Transmit only that data that is absolutely necessary for modeling, intervention and reporting in the public interest, etc.

> 5. Seek equity in the distribution of risks and benefits, minimizing disparate impacts along racial and socio-economic lines, as well as across roles on campus.

Healthcare technology has been particularly criticized for its iniquitous availability and effects (Visser et al. 2018; Weiss et al. 2018; Gonzales 2017). And surveillance technology has been traditionally directed disproportionately at marginalized communities (Nance 2016; Gellman 2017). The intersection of these two technologies could serve as a flashpoint for grave equity concerns, especially when developed and deployed under the time pressures universities now face.

For example, facial recognition systems have well-documented disparities in reliability, depending on the race, skin tone, gender, or age of the person being identified (Associated Press 2019; Henderson 2019).[12] This raises the possibility that people of color (POCs) would be identified less reliably by a covid surveillance system. Thus, they may endure similar risks while being less likely to enjoy the benefits of the system, raising questions of distributive justice with regard to these technologies. We share these and other concerns, which have moved many technology companies to call for regulations—or even a moratorium—on facial recognition technology (Demari 2020). This suggests the technology is in a category all its own, and that universities should approach its use with increased caution, unless its benefits can be shown to be compelling and unobtainable with other means.[13]

Moreover, POCs have been disproportionately affected by the virus already (Golden n.d.; CDC 2020b). Specifically, while false positives raise obvious concerns, false negatives are more serious, and POCs may be less likely to be notified of their potential exposure. When offering students the chance to opt in or opt out of these systems, breakdowns of false positive and false negative rates should be made clear.

Universities should endeavor to ensure that the health and safety of students is not impacted by their race, ethnicity, socioeconomic status, etc. For example, universities should collect multiple modes of contact from students to notify them of potential exposure, in order to respond to the possibility that students might lack reliable Internet access or a mobile phone.

2.2. Process and Governance

6. Thoroughly identify stakeholders and consult with them. At the very least, this likely requires substantive input from students, faculty and staff, and in the surrounding community.

A recurrent failure of technology deployment is a lack of shared governance and input from relevant stakeholders, most often faculty, staff, and students, even when they are the most directly impacted by the technology decisions. Many of these problems—from the threat of disparate impacts to a disturbing lack of consent—could have been identified and pre-empted by ensuring the representation of a wider swath of the affected populations. In many cases, administrative disregard was based on perceived time pressures, or the belief that the stakeholders were not substantially affected. Such assumptions are dangerous and should be avoided. To this point, for example, Zook et al. recommend that data scientists "make grappling with ethical questions part of their standard workflow" (2017, 2)—and consulting with stakeholders early and on an ongoing basis is a crucial part of this. Ballantyne states straightforwardly that "data subjects and communities should have decision-making capacity in relation to data governance and use" (2018, 2).

Consider then extending shared governance principles to data collection and governance policy, in order to anticipate controversies that may arise. Student, faculty, and staff representatives should be involved closely in the decision about how to structure a surveillance strategy, as well as members of the off-campus community, especially when there is frequent student-community interaction. Note that as the norms of data science continue to develop, examining the ethical questions remains the responsibility of practitioners themselves, and should not be shunted onto IRBs or other bodies that have yet to adapt (Zook et al. 2017, 5; Fisk and Hauser 2014; Metcalf and Crawford 2016). Once the ultimate policy is decided upon, its justifications and history of development should be communicated to the community, so that stakeholders can appreciate the balance of tradeoffs and interests that were involved.

7. Consider extending the right to access, audit, and modify data to data subjects.

In the ideal case, the surveillance system would be made accountable, in that data subjects would not just be told that they were surveilled, but would be given access to data about them for the purposes of auditing and correcting mistakes.

This would help minimize what Mittelstadt and Floridi call the "Big Data divide" (2016, 322–23). See, for example:

> The divide can also be conceived in terms of access to modify the data (boyd and Crawford 2012, 674), or whether data subjects are empowered to be notified when data about them are created, modified or analyzed, and given fair opportunities to access the data and correct errors or misinterpretations in the data and knowledge and profiles built upon it (Coll 2014). (Mittelstadt and Floridi 2016, 323)

Calls for this kind of accountability mechanism are motivated by concerns over the autonomy of data subjects, about the ownership of data about oneself, or similarly the "right to be forgotten." All of them, in this instance, are calls for giving data subjects greater control over how data about them are collected and used, in order to level the increasingly pronounced imbalances in power, knowledge, and decision-making privileges between "data-rich" data custodians and "data-poor" data subjects (Mittelstadt and Floridi 2016, 323–24).[14]

2.3. Consent and Coercion

> 8. Explore the possibility of allowing students, faculty, staff, and others to opt out of surveillance.

Universities have a strong prima facie obligation not to surveil their students, faculty, and other community members. Ideally, students and other community members would be able to *opt in* to any surveillance strategy rather than *opt out*, as there are several reasons that count in favor of this. First, asking subjects to opt in is the most reliable way of protecting their privacy, bar none. Second, asking subjects to opt in may be more effective than asking them to opt out. If a student is notified of a positive test result, our understanding is that they will then be required to initiate the contact tracing in any contact tracing app. So, even if students are surveilled and their information shared, they will ultimately have to give their consent for their participation to be valuable, and asking that they opt in may be a more successful way of securing their compliance. Third, any contact tracing scheme is only as useful as the number of people who agree to participate. If a university were to require students to install an app, for example, they would have to make sure that a sufficient number of students had the right brand of cell phone—or a cell phone at all, for that matter! As a referee for this journal correctly pointed out, requiring those kinds of measures could end up disadvantaging historically marginalized groups who are less likely to have the right technology to take part.

Ultimately, these concerns are empirical: what kind of surveillance system is most likely to reach the threshold at which contact tracing is useful for protecting community members, and how much can any system tolerate noncompliers or those who opt out because of reasonable privacy concerns? These are difficult questions to which we do not have the answer, but we acknowledge that there are plausible a priori arguments both for designing these systems as opt-in or opt-out.[15]

On the other hand, there are three strong considerations that count in favor of an opt-out system. First, the behavior of community members has implications for the health and safety of others—*in fact, it entails mortal risks for others, ones that community members are certainly not free to impose on others*, even in the course of achieving worthwhile goals, like getting an education. Second, allowing community members such as students or faculty to opt out of data collection may be practically impossible, as for example in the case of temperature-monitoring CCTVs placed in thoroughfares (though, in that case, robust anonymization would be a necessity). Third, some "critical mass" of participation may be necessary for contact tracing and modeling efforts to be effective at all, as mentioned above. Thus, a presumption in favor of participation, i.e. an opt-out system, may be defensible. See, for example, Ballantyne, who points out that in the public health context, "the coercion of individuals can be justified on the grounds of public interest, but the incursion on individual liberty must be proportional to the anticipated public benefit" (2019, 358). Mittelstadt and Floridi point out that, in some cases,

> explicit, single-instance informed consent is causing rather than solving ethical problems by creating barriers . . . thus preventing researchers from . . . deriving beneficial applications. . . . [While] an opt-out approach to consent should not be seen as ethically equivalent to informed consent . . . a revision of ethical standards which strikes a balance between the requirement for consent and the practical requirements of 'Big Data science' may be appropriate. (2016, 314–15)

It is important to note that we ourselves are somewhat uncomfortable with this conclusion, since we are otherwise staunch proponents of privacy protections. But we cannot deny in this case the pressing and critical public health case for mandatory participation, if it can be secured in a way that is equitable.

There is some debate about whether individual consent and autonomy are the appropriate ethical lenses for understanding the use of health data, especially during emergencies such as the present one (World Medical Association 2016).

Ballantyne (2019) argues, for example, that the more appropriate question is whether such regimes of collection and analysis in the public interest can *outweigh* the violations of individual privacy interests. However, it is clear that universities should exhaust practicable means of securing meaningful individual consent before resorting to justifications that pit data collection or reuse against aggregate social benefits. Because benefits and risks are difficult to measure a priori (Ballantyne 2019, 358), the concern is that universities could simply help themselves to justifications based on speculative or vague claims about the public benefit.

Universities should explore alternative models of securing consent that balance autonomy and privacy against the practical realities of needing data to derive valuable insights at all.[16] Still, universities should also investigate the possibility of operating with less than perfect knowledge about all community members, e.g., by allowing them to opt out, or by placing limitations on the knowledge gathered. Finally, note that much turns on the question of whether universities design their systems as opt-in or opt-out systems, since most people will stick with the "default setting" (Shah and Sandvig 2008; Thaler and Sunstein 2009).

> 9. Notify community members of the details of the surveillance strategy, especially if opting out is not possible.

The risk to each individual differs with their life circumstances: their health status (for example, underlying conditions and comorbidities, or possible immunity from a previous infection), their living situation, contact with relatives or the community, etc. The best way to acknowledge this is education: to make people aware whenever possible of the risks of the disease and the contours of the surveillance strategy, and then give them the opportunity to opt out. Only in such an information environment can universities sincerely say they have secured meaningful consent from their community members to surveillance. On this note, Ballantyne says,

> Full transparency [required for meaningful consent] would include a public description of the data activity, purpose and justification, anticipated social value, harm-mitigation strategies, public engagement strategies, level of security and encryption, research results, and the coding/algorithms. (2018, 3)

At the very least, universities must inform students, faculty, staff, etc., that their presence on campus will entail surveillance and data collection of whatever forms: e.g. financial, health, location, faceprint and temperature, etc. In this case, students may choose to defer their in-person education until the pandemic passes, and others may choose to modify their behavior in order to avoid being subject to

surveillance. Relatedly, universities must strive to make virtual education or distance learning as effective, inclusive, and engaging as in-person classes to reduce the educational cost of staying off campus. If students feel they make a genuine sacrifice by taking virtual courses, they will be more willing to risk their health to pursue their education in person.

Extensive efforts should be made to publicize the introduction of any surveillance strategy, ensuring that as many students as possible are aware of its introduction before it is implemented. Consider recruiting and training dedicated 'privacy liaisons' for each college or unit to act as points of contact for students, faculty, and staff with questions or concerns about their privacy. Consider means of distinguishing crucial notices about health surveillance from routine emails about campus events or other comparatively trivial matters. This also suggests plastering relevant information on the university website, learning management systems, email signatures of faculty, staff, and administration, imposing modal click-through dialogues before registering for courses, and so on.

10. Keep data operations in-house as much as possible.

Keeping data operations in-house would help to avoid the question of data transfer entirely. Otherwise, universities risk becoming ensnared with companies whose data practices may be more lax. This may preclude Google Cloud, Amazon Web Services, or other companies located in different states (or countries) whose data protection practices might differ dramatically.[17] In the past, our team has been aghast at the privacy policies of third-party vendors contracting with our institution, including their failure to abide by simple industry best practices, i.e. Fair Information Practices (FIPs) (OECD 2013).

3. Conclusion

Many further challenges will confront universities in the current and coming academic terms; the suggestions above should be taken only as a starting point. Concern has swelled, driven by the recent implementation of other surveillance technologies (Harwell 2019a; Witz 2019). Bans on facial recognition technologies, for example, already have been implemented at several prominent universities (Fight for the Future 2020, n.d.). Universities should be prepared to face significant pushback and skepticism about their surveillance strategies, while simultaneously contending with the maddening contagions of misinformation and conspiracy theories concerning the disease.

We have left out many other issues that colleges must consider, which fall more squarely within the purview of public health ethics. Even after campuses have reopened, universities must ensure that continuing and new safety measures are ethically responsible, including examining "sunset" provisions or phased reopenings.

The use of technologies that many find invasive and dystopian threatens to erode further the mutual respect that is necessary to support healthy learning environments. Again, the purpose of grappling with ethical questions is not to arrive at the 'one best way' of implementing a solution, but rather to equip oneself with an explicit and thoughtful justification for the tradeoffs that are necessary, and to be able to "articulate the tradeoffs . . . as publicly and transparently as possible" (Ballantyne 2018, 3). By providing empirically grounded and ethically sensitive best practices, we hope to provide the resources for universities to make a good faith effort in deploying these technologies in ways that can augment safety without eroding trust and inviting criticism, skepticism, or noncompliance.

Acknowledgments

The authors would like to thank the members of the Ethics + Emerging Sciences Group at Cal Poly, namely Pat Lin and Bruce DeBruhl. Thanks are also owed to Parker Ornellas and David McCullough who helped with background research. Two anonymous reviewers for this journal provided helpful comments, through which the paper has been much improved. This work was supported by NSF award #1917707, "Artificial Intelligence and Predictive Policing: An Ethical Analysis."

Notes

1. That is, universities are applying the techniques of Big Data to solve the problem. Big Data, say Mittelstadt and Floridi (2016, 309), "is unique in terms of the size and 'speed of data generation and processing and the heterogeneity of data that can be dumped into combined databases' (Andrejevic 2014, 1676)."
2. This idea was floated to one of the authors in conversation.
3. As Mittelstadt and Floridi (2016, 305f.) point out, "biomedical Big Data has gained significant attention due to a combination of two factors. One the one hand, there is the huge potential to advance diagnosis, treatment, and prevention of diseases as well as foster healthy habits and practices (Costa 2014). On the other hand, there is the obvious, inherent sensitivity of health-related data and the implicit vulnerability and needs of those potentially requiring treatments (Pellegrino and Thomasma 1993)." Interestingly, the suggestions considered here, specifically, "involuntary linked online/

offline surveillance," was contemplated by Mittelstadt and Floridi, but was labeled "not currently possible" when they were writing (2016, 311).

4. Moreover, the suggestions we make here have a broad relevance to other applications of surveillance in other domains, for example, the future of the classroom and the use of "lockdown" test-proctoring applications like Respondus, the use of surveillance in K–12 schools, workplace surveillance, etc.

5. We follow Mittelstadt and Floridi's choice of terminology, which the data ethics community seems to be coalescing around: "'data subject' refers to the individual described by the data, 'data custodian' refers to any individual or organization responsible for hosting or archiving the data in either its individual or aggregated form, and 'data analyst' refers to any individual or organization analyzing the data, but not necessarily hosting it" (2016, 308).

6. Our common language seems to lack the tools to describe and understand actions that are not outright privacy violations, but do transgress some implicit social norms. In our experience, people often resort to describing these actions as "creepy." For example, when students are confronted with the knowledge that the University logs their location data, students might react, "Well, I suppose they have the *right* to that information, but it's still *creepy*." See also Zook et al. 2017, 3.

7. Both of these are American laws that control the release of sensitive information. The Federal Family Educational Rights and Privacy Act of 1974 (FERPA) controls the release of educational information, such as a student's grades. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) governs the dissemination of medical information. Both of these laws have implications for how universities handle information about students' personal information and health records, and universities under their jurisdictions should heed their requirements, which can be stringent. We suspect that universities in European and other countries would certainly have analogous legal requirements to abide by.

8. This is to say nothing of the significant technical concerns with contact-tracing apps, for example, that they will have unacceptable rates of false positives and false negatives, effectively rendering them useless. See the influential Bruce Schneier (2020) on this point.

9. For what it is worth, there is relatively little work we could find, so far, on other approaches to preserving privacy in tracking covid, such as differential privacy or federated learning. See, for one example, Hyunghoon Cho et al. in preprint (2020).

10. For example, "Immigration and Customs Enforcement (ICE) officials employed facial recognition technology to scan motorists' photos to identify undocumented immigrants" (Metz 2019) and have used such databases as a "gold mine" to form "the bedrock of an unprecedented surveillance infrastructure" (Harwell 2019a)—not to search for wanted fugitives, but simply people trying to go about their lives.

11. See also Christopher A. Bail (2014) and especially Lawrence Busch (2014) which discuss in detail the aspects of Big Data that can lead to de-contextualization, notably, that "aspects of things that are not amenable to numerical or statistical analysis . . . are systematically downgraded or removed from consideration" (Busch 2014, 1735).

12. The technical reasons for this are not relevant for our discussion.

13. We thank an anonymous referee for this journal for suggesting that we highlight the extraordinary concerns with facial recognition technologies.

14. See also the same authors: "Considered together, the emerging picture is of data subjects in a disempowered state, faced with seemingly insurmountable barriers to understanding *who* holds *what* data about them, being used for *which* purposes. Further, in relation to modification and correction of personal data, it is unclear how subjects can possibly propose changes to data without first understanding the contents and inferences drawn from them, or the perhaps inaccurate or incomplete ways in which the data represent the subject and her behaviors" (2016, 330).

15. Also, whether these systems *can* be implemented as opt-in or opt-out hinges on the details and application of the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act (HIPAA), and whether universities will be legally permitted to collect this information, share it, and with whom, before students explicitly opt in. We will leave those questions to university compliance units and restrict ourselves to considering what we think is a strong ethical case for designing these systems as opt-out.

16. Mittelstadt and Floridi helpfully survey several alternative models of securing consent that universities should consider (2016, 312–16).

17. Moreover, using third-party services to store these sensitive data could be in violation of HIPAA or FERPA, and thus complicate compliance efforts (or frustrate them entirely). We are grateful to an anonymous referee for this journal for pointing out this important complication.

References

Andrejevic, Mark. 2014. "The Big Data Divide." *International Journal of Communication* 8.

Apple, Inc. n.d. "Privacy-Preserving Contact Tracing—Apple and Google." *Apple*. Accessed June 27, 2020. https://www.apple.com/covid19/contacttracing.

Associated Press. 2019. "Federal study finds race, gender bias in facial recognition technology." *USA Today*. December 19, 2019. https://www.usatoday.com/story/tech/2019/12/19/facial-recognition-study-finds-results-biased-race-gender-and-age/2704291001/.

Auxer, Brooke, and Lee Rainie. 2019. "Key Takeaways on Americans' Views about Privacy, Surveillance and Data-Sharing." *Pew Research Center*. November 15, 2019. https://www.pewresearch.org/fact-tank/2019/11/15/key-takeaways-on-americans-views-about-privacy-surveillance-and-data-sharing/.

Bail, Christopher A. 2014. "The Cultural Environment: Measuring Culture with Big Data." *Theory and Society* 43(3–4): 465–82. https://doi.org/10.1007/s11186-014-9216-5

Ballantyne, Angela. 2018. "Where Is the Human in the Data? A Guide to Ethical Data Use." *GigaScience* 7(7): giy076. https://doi.org/10.1093/gigascience/giy076

Ballantyne, Angela. 2019. "Adjusting the Focus: A Public Health Ethics Approach to Data Research." *Bioethics* 33(3): 357–66. https://doi.org/10.1111/bioe.12551

boyd, danah, and Kate Crawford. 2012. "Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon." *Information, Communication & Society* 15(5): 662–79. https://doi.org/10.1080/1369118X.2012.678878

Burke, Lilah. 2020. "Monitoring Vital Signs for COVID-19." *Inside Higher Ed*. Accessed August 24, 2020. https://www.insidehighered.com/news/2020/08/11/university-use-wearable-tech-track-covid-campus.

Busch, Lawrence. 2014. "A Dozen Ways to Get Lost in Translation: Inherent Challenges in Large Scale Data Sets." *International Journal of Communication* 8.

Calo, Ryan. 2011. "The Boundaries of Privacy Harm." *Indiana Law Journal* 86: 1131.

CDC. 2020a. "Coronavirus Disease 2019 (COVID-19)—Symptoms." *Centers for Disease Control and Prevention*. May 13, 2020. https://www.cdc.gov/coronavirus/2019-ncov/symptoms-testing/symptoms.html.

CDC. 2020b. "COVID-19 in Racial and Ethnic Minority Groups." *Centers for Disease Control and Prevention*. February 11, 2020. https://www.cdc.gov/coronavirus/2019-ncov/need-extra-precautions/racial-ethnic-minorities.html.

Cho, Hyunghoon, Daphne Ippolito, and Yun William Yu. 2020. "Contact Tracing Mobile Apps for COVID-19: Privacy Considerations and Related Trade-Offs." arXiv preprint arXiv:2003.11511.

Coll, Sami. 2014. "Power, Knowledge, and the Subjects of Privacy: Understanding Privacy as the Ally of Surveillance." *Information, Communication & Society* 17(10): 1250–63. https://doi.org/10.1080/1369118X.2014.918636

Costa, Fabricio F. 2014. "Big Data in Biomedicine." *Drug Discovery Today* 19(4): 433–40. https://doi.org/10.1016/j.drudis.2013.10.012

Criddle, Cristina, and Leo Kelion. 2020. "Coronavirus Contact-Tracing: World Split between Two Types of App." *BBC News*. May 7, 2020, sec. Technology. https://www.bbc.com/news/technology-52355028.

Crocker, Andrew, Kurt Opsahl, and Bennett Cyphers. 2020. "The Challenge of Proximity Apps For COVID-19 Contact Tracing." *Electronic Frontier Foundation*.

April 10, 2020. Accessed February 25, 2021. www.eff.org/deeplinks/2020/04/challenge-proximity-apps-covid-19-contact-tracing.

Fight for the Future. 2020. "New Scorecard Shows Which Colleges Are Using Facial Recognition, and Which Say They Won't." *Common Dreams*. January 28, 2020. Accessed June 27, 2020. https://www.commondreams.org/newswire/2020/01/28/new-scorecard-shows-which-colleges-are-using-facial-recognition-and-which-say.

Fight for the Future. n.d. "Stop Facial Recognition on Campus." Accessed June 27, 2020. https://www.banfacialrecognition.com/campus/.

Floridi, Luciano. 2020. "Mind the App: Considerations on the Ethical Risks of COVID-19 Apps." *Philosophy & Technology* 33: 167–72. https://doi.org/10.1007/s13347-020-00408-5

Gellman, Barton. 2017. "The Disparate Impact of Surveillance." *The Century Foundation.* December 21, 2017. https://tcf.org/content/report/disparate-impact-surveillance/.

Gitlin, Jonathan M. 2020. "More than 7 in 10 Americans Won't Use Contact-Tracing Apps, Data Shows." *Ars Technica*. June 15, 2020. https://arstechnica.com/science/2020/06/more-than-7-in-10-americans-dont-want-contact-tracing-data-shows/.

Golden, Sherita. n.d. "Coronavirus in African Americans and Other People of Color." *Johns Hopkins Medicine*. Accessed June 27, 2020. https://www.hopkinsmedicine.org/health/conditions-and-diseases/coronavirus/covid19-racial-disparities.

Gonzales, Amy. 2017. "Is Digital Technology Making Health Inequality Worse?" *IAPHS—Interdisciplinary Association for Population Health Science* (blog). November 20, 2017. https://iaphs.org/digital-technology-making-health-inequality-worse/

Harwell, Drew. 2019a. "Colleges Are Turning Students' Phones into Surveillance Machines." *The Washington Post*. December 24, 2019. https://www.washingtonpost.com/.

Harwell, Drew. 2019b. "FBI, ICE Find State Driver's License Photos Are a Gold Mine for Facial-Recognition Searches." *The Washington Post*. July 7, 2019. https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/.

Heilweil, Rebecca. 2020. "The Dystopian Tech That Companies Are Selling to Help Schools Reopen Sooner." *Vox*. August 14, 2020. https://www.vox.com/recode/2020/8/14/21365300/artificial-intelligence-ai-school-reopening-technology-covid-19.

Henderson, Sarah. 2019. "NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software." *NIST*. December 19, 2019. https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software.

Hern, Alex. 2019. "'Anonymised' Data Can Never Be Totally Anonymous, Says Study." *The Guardian*. July 23, 2019, sec. Technology. https://www.theguardian.com/technology/2019/jul/23/anonymised-data-never-be-anonymous-enough-study-finds.

Institute for Ethics in Artificial Intelligence (IEAI). 2020. "Ethics and the Use of AI-based Tracing Tools to Manage the COVID-19 Pandemic." *Technical University of Munich. Munich Center for Technology in Society Institute for Ethics in Artificial Intelligence*. Research Brief. June 2020. https://ieai.mcts.tum.de/wp-content/uploads/2020/06/Research-Brief_ContactTracingAppsFinal.pdf.

Jargon, Julie. 2020. "Back to School? Look Out for Covid-Tracking Surveillance Tech." *The Wall Street Journal*. August 11, 2020. https://www.wsj.com/articles/back-to-school-look-out-for-covid-tracking-surveillance-tech-11597150800.

Knight, Will. 2020. "Schools Turn to Surveillance Tech to Prevent Covid-19 Spread." *WIRED*. June 5, 2020. https://www.wired.com/story/schools-surveillance-tech-prevent-covid-19-spread/.

Lewis-Kraus, Gideon. 2018. "Facebook and the 'Dead Body' Problem." *The New York Times*. April 24, 2018. https://www.nytimes.com/2018/04/24/magazine/facebook-and-the-dead-body-problem.html.

Markham, Annette. 2016. "OKCupid data release fiasco: it's time to rethink ethics education." *Points*. May 18, 2016. Accessed September 25, 2020. https://points.datasociety.net/okcupid-data-release-fiasco-ba0388348cd.

Marwick, Alice E., and danah boyd. 2014. "Networked Privacy: How Teenagers Negotiate Context in Social Media." *New Media & Society* 16(7): 1051–67. https://doi.org/10.1177/1461444814543995

Metcalf, Jacob, and Kate Crawford. 2016. "Where Are Human Subjects in Big Data Research? The Emerging Ethics Divide." *Big Data & Society* 3(1): 1–14. https://doi.org/10.1177/2053951716650211

Metz, Cade. 2019. "Facial Recognition Tech Is Growing Stronger, Thanks to Your Face." *The New York Times*. July 13, 2019, sec. Technology. https://www.nytimes.com/2019/07/13/technology/databases-faces-facial-recognition-technology.html.

Miller, Michael. 2020. "WVXU: How Drones Can Slow Spread of COVID-19." *UC News*. May 26, 2020. https://uc.edu/news/articles/2020/05/n20918352.html.

Mittelstadt, Brent Daniel, and Luciano Floridi. 2016. "The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts." *Science and Engineering Ethics* 22(2): 303–41. https://doi.org/10.1007/s11948-015-9652-2

Morley, Jessica, Josh Cowls, Mariarosaria Taddeo, and Luciano Floridi. 2020. "Ethical Guidelines for SARS-CoV-2 Digital Tracking and Tracing Systems." *SSRN* Scholarly Paper. April 22, 2020. https://papers.ssrn.com/abstract=3582550. https://doi.org/10.2139/ssrn.3582550

Nance, Jason P. 2016. "Student Surveillance, Racial Inequalities, and Implicit Racial Bias." *Emory Law Journal* 66: 765.

Nissenbaum, Helen. 2004. "Privacy as Contextual Integrity." *Washington Law Review* 79(1): 119.

Nissenbaum, Helen. 2009. *Privacy in context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford University Press. https://doi.org/10.1515/9780804772891

Nissenbaum, Helen. 2011. "A Contextual Approach to Privacy Online." *Daedalus* 140(4): 32–48. https://doi.org/10.1162/DAED_a_00113

O'Doherty, Kieran, Emily Christofides, Jeffery Yen, Heidi Bentzen, Wylie Burke, Nina Hallowell, Barbara Koenig, and Don Willison. 2016. "If You Build It, They Will Come: Unintended Future Uses of Organised Health Data Collections." *BMC Medical Ethics* 17: 54. https://doi.org/10.1186/s12910-016-0137-x

OECD. 2013. "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data." https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

Pellegrino, Edmund D., and David C. Thomasma. 1993. *The Virtues in Medical Practice*. New York: Oxford University Press.

Roxby, Philippa. 2020. "Can You Really Spot the Virus from an Image like This?" *BBC News*. June 9, 2020, sec. Health. https://www.bbc.com/news/health-52940951.

Schneier, Bruce. 2007. "Why 'Anonymous' Data Sometimes Isn't." *WIRED*. December 12, 2007. https://www.wired.com/2007/12/why-anonymous-data-sometimes-isnt/.

Schneier, Bruce. 2020. "Me on COVID-19 Contact Tracing Apps." *Schneier on Security*. Accessed October 19, 2020. https://www.schneier.com/blog/archives/2020/05/me_on_covad-19_.html.

Shah, Rajiv C., and Christian Sandvig. 2008. "Software Defaults as De Facto Regulation: The Case of the Wireless Internet." *Information, Community & Society* 11(1): 25–46. https://doi.org/10.1080/13691180701858836

Thaler, Richard H., and Cass R. Sunstein. 2009. *Nudge: Improving Decisions About Health, Wealth, and Happiness.* London: Penguin Books.

Tzachor, Asaf, Jess Whittlestone, Lalitha Sundaram, and Seán Ó hÉigeartaigh. 2020. "Artificial Intelligence in a Crisis Needs Ethics with Urgency." *Nature Machine Intelligence* 2(3): 365–66. https://doi.org/10.1038/s42256-020-0195-0

Visser, Laura M., Yvonne W. M. Benschop, Inge L. Bleijenbergh, and Allard C. R. van Riel. 2018. "Unequal Consumers: Consumerist Healthcare Technologies and Their Creation of New Inequalities." *Organization Studies*. May 18, 2018. https://doi.org/10.1177/0170840618772599

Weiss, Daniel, Håvard T. Rydland, Emil Øversveen, Magnus Rom Jensen, Solvor Solhaug, and Steinar Krokstad. 2018. "Innovative Technologies and Social

Inequalities in Health: A Scoping Review of the Literature." *PLoS ONE* 13(4): e0195447. https://doi.org/10.1371/journal.pone.0195447

Witz, Billy. 2019. "Orwellabama? Crimson Tide Track Locations to Keep Students at Games." *The New York Times*. September 12, 2019. https://www.nytimes.com/2019/09/12/sports/alabama-tracking-app.html.

World Health Organization. 2017. "Policy on use and sharing of data collected in Member States by the World Health Organization (WHO) outside the context of public health emergencies." August 22, 2017. Available at https://www.who.int/publishing/datapolicy/Policy_data_sharing_non_emergency_final.pdf.

World Medical Association. (2002) 2016. "WMA Declaration of taipei on ethical considerations regarding health databases and biobanks." WMA's policies on ethical and social issues. Accessed February 2, 2020. https://www.wma.net/policies-post/wma-declaration-of-taipei-on-ethical-considerations-regarding-health-databases-and-biobanks/.

Zook, Matthew, Solon Barocas, danah boyd, Kate Crawford, Emily Keller, Seeta Pena Gangadharan, Alyssa Goodman, Rachelle Hollander, Barbara A. Koenig, Jacob Metcalf, Arvind Narayanan, Alondra Nelson, and Frank Pasquale. 2017. "Ten simple rules for responsible big data research." *PLoS Comput Biol* 13(3): e1005399. https://doi.org/10.1371/journal.pcbi.1005399