5

Surveillance and Human Flourishing

Pandemic Challenges

David Lyon

For humans to flourish in a digital world, three emerging issues should be addressed, each of which was amplified by the global Coronavirus pandemic of 2020–2022. The first is that the use of data to solve human problems is frequently compromised by the failure to understand the character of the "human" problems at hand. Rather than seeing this only in relation to the pandemic, the second issue is to acknowledge that a key factor informing and galvanizing "datafied" responses is the role of surveillance capitalism, whose emergence predated the pandemic. Shoshana Zuboff (2019) highlights some "human" consequences of this phenomenon. The third issue is to retrieve some sense of what "human flourishing" might mean, specifically as it relates to surveillance, and how this might affect *how* surveillance is done. For this, Eric Stoddart's (2021) notion of the "common gaze" is briefly discussed as a starting point.

5.1 HUMAN PROBLEMS, SURVEILLANT RESPONSES: THE COVID-19 PANDEMIC

The Coronavirus pandemic that began in 2020 broke out in a *digital* world. This context is significant because, like the virus itself, it was novel. Even SARS in 2002 or H1N1 in 2009 did not occur in conditions that were recognized as "surveillance capitalism," although the seeds of that conjunction were already sown (Mosco 2014; Zuboff 2015). It is important because widespread "datafication" was increasingly characterized by *dataism*, "the widespread *belief* in the objective quantification and potential tracking of all kinds of human behaviour and sociality through online media technologies" (van Dijck 2014, 198). Described in several other venues as having "religious" qualities, dataism accompanies descriptions of "Big Data" and further catalyzes phenomena such as "tech solutionism," in which digital technology, that is, based in computing sciences, is assumed to be *the* answer to human problems, prior to any full understanding of the problem in question (Mozorov 2013).

Dataism, that was clearly evident in the "security" responses to 9/11, ballooned once again worldwide in 2020–2021 as a crucial response to the global pandemic. It is

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 17:17:18, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009383851.006

visible in the massive turn to apps, devices, and networked data systems that occurred as soon as the pandemic was recognized as such by the WHO in March 2020. Public health data, clearly believed to be vital to the accurate assessment and prediction of trends, was used to track the course of the virus, apps were developed to assist in the essential task of contact-tracing, and devices from wearables to drones were launched as means of policing quarantine and isolation. At the same time, other surveillant systems also expanded rapidly, not just to provide platforms to connect those obliged to remain at home but also to monitor the activities of working, learning, and shopping from home, thus sucking them into the gravitational field of surveillance capitalism. And as well, some started to suspect that all this digital activity would not dissipate once the pandemic was over; government, healthcare, and commerce would entrench the new surveillant affordances within their organizations on a permanent basis (Lyon 2022b).

Thus, dataveillance, or surveillance-using-data,[1] received an unprecedented boost during the COVID-19 pandemic, and, though unevenly distributed, on a global level. Its impact – positive and negative – on human flourishing was widespread. Positively, it is reported that dataveillance permitted relatively rapid information about pandemic conditions to reach citizens in each locale. Negatively, in the name of accelerating pandemic responses, some liberties were taken with data use, that had effects including diminishing the responsibility of data-holders to so-called data-subjects, the human beings whose activities produce the data in the first place.

In Ontario, Canada, for instance, privacy laws purportedly designed to provide citizens with control over the surveillance technologies that watch them, were modified to allow for new access to public health data by commercial entities to enable better statistical understanding of the pandemic, and the definition of "deidentification" of data was also changed to allow for new technological developments, even though the ability of data analytics to *re*identify such data is also expanding (Scassa 2020). This allowed, for example, for new levels of data integration on the Ontario Health Data Platform, which was newly established in 2020 to "detect, plan and respond to the COVID-19 outbreak."[2] Such changes were minor, however, when compared with similar activities in some other countries.

5.2 PUBLIC HEALTH DATAVEILLANCE

In January 2020, someone infected with COVID-19 criss-crossed the city of Nanjing, China, on public transit, risking infection to many others en route. Authorities were

[1] Surveillance occurs by many means. Human ocular vision for surveillance has been augmented mechanically, especially from the nineteenth century and digitally, from the later twentieth, in order to make lives "visible" to those seeking such information.

[2] Ontario Health. www.ontariohealth.ca/public-reporting/open-data.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 17:17:18, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009383851.006

able to track the person's route, minute-by-minute, from the subway journey record. Details were published on social media with warnings to others on the route to be checked. Facial recognition, security cameras, and social media plus neighbourhood monitors and residential complex managers, together add up to an impressive surveillance arsenal, quickly adapted for the pandemic. A patient in Zhejiang province denied having had contact with anyone from Wuhan, but data analysis revealed contacts with at least three such persons. When cellphones are linked with national ID numbers, officials can easily make connections. But ordinary citizens can also use, for example, digital maps for checking retrospectively if they were near known infected persons (Chin and Lin 2022). Some privacy has to be sacrificed in such an emergency, so Chinese lawyers argue (Lin 2020).

But such trade-offs significantly shift the experience of being human in the digital world. They suggest that some circumstances demand that normal (at least in liberal democracies) expectations of privacy or data protection be downplayed or denied in favour of technocratic institutional control. In the case of the pandemic, where panicked responses seem common, such demands are often made in haste. Moreover, the lack of transparency – such as obscuring significant changes in catch-all legislative action make it even harder to both identify and resist the constraints placed on humans as objects in the data system. Some obvious objections that could be raised relate to the risks of rapidly adding new dimensions to surveillance and to the fact that, lacking clear and respected sunset clauses, such changes may settle and solidify into longer-term laws. After all, just such patterns occurred following 9/11, that proved to be permanent "states of exception," especially in the United States (Ip 2013).

However, trade-offs also give the impression that some aspects of human life are at least temporarily dispensable for some greater good. But this is surely a very questionable if not dangerous assumption, given that many of the technologies mobilized against the virus are relatively untested, with unproven benefits, and that the risks they present to society may be considerable, and long-term. As Rob Kitchin (2020, 1) argued, early in the pandemic, the mantra should not be "public health *or* civil liberties" but both, and simultaneously. Of course, great efforts should be made to reduce the scourge of a global pandemic that causes so much human suffering and death. But health is just one feature of human flourishing – freedom from undue government interference or a sense of fairness in everyday social arrangements being two others. It would certainly be odd for a government to argue that, while strenuous efforts are made to ensure freedom and equality, public healthcare concerns will be suspended or reduced.

This draws attention to the value of an over-arching sense of the significant conditions for human flourishing. So, it is worth considering carefully what substantial aspects of being human should be underscored in a digital era. In what follows I touch on some that were historically relevant, a generation ago, as well as some sparked by today's pandemic context. The technology was far less developed – the

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 17:17:18, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009383851.006

word "digital" was not used with today's frequency for instance – and the specific example pre-dates today's "autonomous vehicles."

Jeff Reiman's (1995) thoughtful discussion of the "Intelligent Vehicle Highway System (IVHS)" in *Driving to the Panopticon*, for example, drew attention to the fact that surveillance not only makes people visible but does so from a single point. What a contrast with today's surveillance situation, where corporations gather data promiscuously from "public" or "private" sources to identify and profile us from multiple points! So, for him, 30 years ago, privacy protection was not merely about "strengthening windows and doors," he said, but about remembering that information collection is about gathering pieces of our public lives and making them visible from a single point. It is almost quaint to recall that Reiman considered privacy as "the condition in which others are deprived of access to you," something he regarded as a right (1995, 30). However, Reiman's instincts were admirable. He was not toying with ideas about how drivers of "intelligent vehicles" might wish to restrict access to their personal data in ways that might disadvantage them as consumers but asking what possible consequences of such vehicle-use might mean for human dignity.

Reiman (1995) reminded readers that the IVHS did not exist in an information vacuum but in relation to a "whole complex of information" gathering from many government departments and organizations that he thought of as an "informational panopticon." This challenges, he avers, both extrinsic and intrinsic freedom, symbolic risks, and even what he called "psycho-political metamorphosis" (Reiman 1995, 40). In this last, he pondered a surveillance future in which humans become less noble, interesting, and worthy of respect – deprived of dignity. "As more of your inner life is made sense of from without," Reiman wrote, ". . . the need to make your own sense out of your inner life shrinks" (Reiman 1995, 41). But that same healthy inner life is required for political life, in a democracy, and for judging between different political parties or policy options. The risks of privacy – the lack that comes from knowing that one is visible to unknown others – arise from datafied systems often set up for what were believed to be beneficent purposes.

Reiman argued that while one needs *formal* conditions for privacy – such as rights – one also needs *material* conditions, by which I think he means systems that are privacy protective by design and operation precisely because they are an essential part of an environment that allows humans to exercise agency and experience dignity. Perhaps because he was writing a generation ago, his comments now seem almost quaint, and yet strangely relevant. Quaint because they antedate the Internet in its interactive phase, social media, and surveillance capitalism. And relevant in an even more urgent way, because of what happens when global pandemics – or other global crises – are unleashed on a world of already existing surveillance capitalism.

The COVID-19 pandemic was marked by a dataism-inspired celebration of tech solutionism by *both* corporate *and* government actors, often, seemingly willing to play down the impact of the "privacy" implications of technical and legal shifts on the human beings in the system. And relevant, too, in a world of social media in

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 17:17:18, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009383851.006

which the platforms' profit motive not only colonizes further the "inner life," but also undermines previous democratic practice, as the same profit-oriented social media boost political polarization and simultaneously threaten social justice, doing so with apparent impunity. Each of these is a threat to human flourishing.

Many thoughtful people sense that some larger questions have to be answered to ensure that humans living in the emerging surveillance system can thrive, rather than merely working within the more familiar frames of privacy and data protection, valuable though those have been and still are. For me, as someone who has been working in Surveillance Studies more-or-less since its inception (in the 1990s[3]), I have found much inspiration among those who frame the issues – and thus the critical analysis of the human impact in actual empirical situations – in terms of data ethics in general and data justice in particular. This is consonant with my own long-term quest to understand, for example, the "social sorting" dynamics of much if not all surveillance today.

Such sorting scores and ranks individuals within arcane categories, leading to differential treatment (Lyon 2003). They profoundly affect *human* life. Such practices are common to all forms of surveillance, from commercial marketing to policing and government. They unavoidably affect, in other words, everyday human life in multiple contexts. Many cite so-called social credit systems in China as extreme examples of such social sorting by government departments, in tandem with well-known major corporations (Chin and Lin 2022). However, while few governments enjoy the direct use and control of sorting systems – combined, in the Chinese and a few other cases, with the use of informers and spies (e.g. Pei 2021) –such sorting is carried out constantly in countries around the world with more random but no less potentially negative results. This is exacerbated today by the increasing use of AI, whose algorithms are often distorted from the outset by inadequate machine learning due to poor data sources. Black and poorer people in the United States, for instance, suffer systematic discrimination when sorting outcomes depend in part on AI. A striking case is that of facial recognition systems, that are notoriously limited in their capacity to distinguish major categories of targets. Joy Buolamwini, whose PhD at the Massachusetts Institute of Technology demonstrated failures of facial recognition systems, especially in the case of black women, took it upon herself to found the Algorithmic Justice League, in response. She speaks explicitly of "protecting the human" from negative effects of AI (Buolamwini 2022).

So while, 30 years ago, Reiman's (1995) concern for the "inner life" in intensifying surveillance conditions was justified – compare Zuboff's (2019) critique of such "inner" manipulation via surveillance capitalism – today's surveillance equally

[3] The 1990s was when the term "surveillance studies" began to be used. A number of authors had started *doing* surveillance studies at least from the 1970s, with Michel Foucault's historical investigations, or James Rule's more empirical sociology – earlier if one includes the work of Hannah Arendt. See e.g. Xavier Marquez's (2012) *Spaces of Appearance and Spaces of Surveillance* and David Lyon's (2022a) *Reflections on 40 Years of Surveillance Studies*.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 17:17:18, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009383851.006

affects the "outer life" of material conditions, of social disadvantage, by means of social sorting, dubious data-handling methods, biased algorithms, and so on (Cinnamon 2017). Let me comment on the work of Linnet Taylor (2017), as a starting point for discussion, before taking this further, using other pandemic surveillance challenges to point to a larger context within which people's "inner" and "outer" lives might be placed.

With respect to the pandemic, Taylor (2020) observes that data is far from certain – even death rates are hard to calculate accurately – and yet are often treated as accurate and objective proxies for human experiences and understandings (due, arguably, to data's status-inflation in data*ism*). Thus, she turns to an ethics of care, that is embodied, that takes account of what can be known about the person within the system, and considers problems to be overcome from there. People are seen as collectives, bound by responsibilities to others, not as mere data points defined by their responses to rational incentives.

This prompts a quest for understanding those people made invisible or out of focus by official statistics – the elderly-in-care, prisoners, migrant workers, and the like, each of whom have their own reasons for mobility, or lack thereof, among other pandemic-related factors. Much "pandemic data" was created by policy, rather than vice versa. Thus, as Taylor shows, even reducing the number of deaths can become a policy target, in some circumstances, as occurred under President Trump in his first term. He proposed to keep deaths under 100,000 in a highly instrumental fashion, that allowed for data-collection practices that confirmed the goal. This was similar to Boris Johnson's efforts in the United Kingdom, to make a "herd immunity policy" in warning of untimely deaths but not restricting the size of public gatherings. The dynamics of data collection and use are very uneven and work to obscure the human aspects of the problems that data are being mobilized to solve. As Taylor (2020) says, "statistical normality is abnormal – it is the minority position. There is no 'herd,' only a mosaic of different vulnerabilities" that are experienced in the context of each human life.

Such a perspective builds on one of Linnet Taylor's (2017) earlier contributions, on data justice. The granular data sources enabling companies and government departments to sort, categorize, and intervene in people's lives are seldom yoked with a social justice agenda. Especially among marginalized groups, distributed visibility has consequences. In *What Is Data Justice? The Case for Connecting Digital Rights and Freedoms Globally*, Taylor (2017) carefully outlines various approaches to data justice and proposes that it may be defined as "fairness in the way people are made visible, represented and treated as a result of the production of digital data." She also outlines three "pillars" of data justice, building on case-studies and discussions of the theme around the world. They are (in)visibility, (dis)engagement with technology, and antidiscrimination (Taylor 2017). And she pleads not merely for "responsible" but for "accountable" technology, that, arguably, would make transparency and therefore trust much more meaningful realities.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 17:17:18, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009383851.006

These reflections on the "pandemic challenges" to questions of surveillance and human flourishing certainly go beyond what Reiman was arguing in the mid-1990s and yet they still resonate with his core argument about the challenges to *humanness* in what was then termed a time of "information technology." Today's challenge is to confront the *data-driven* character of surveillance, that in turn is strongly associated with the profit-driven activities of surveillance capitalism, now deeply implicated in responses to the COVID-19 pandemic. People are now made visible in ways which Reiman did not even dream. And these have consequences that relate not only to the potential power of government along with the erosion of the "inner life," but also to the production and reproduction of social inequalities, both local and global. People are "made visible, represented and treated" by surveillance and such activities demand viable ethical practices suited to each human context.

The global COVID-19 pandemic demonstrated the need for data justice and data ethics in new and stark ways, again, both locally and globally. Never before has so much information circulated, accurately or otherwise, about a pandemic and never before has so much attention been paid to those data-driven statistics. No doubt, within the swirling data currents, some accurate and helpful moves have been made in public health. But, all-too-often, the lines of familiar, historical disadvantage have been traced once more, sometimes reinforcing their hold.

Vulnerability is surely linked with the use of Big Data, a term more often associated with the merely technical "Vs" of volume, velocity, and variety. This applies to rich countries like Canada as well as much poorer ones, such as India. In others, such as China, it is harder to tell just how far pandemic surveillance more effectively alleviated the contagion – although the social costs of this were high (see e.g. Ollier-Malaterre 2024; Xuecun 2023). Arguably, in a more *human* world, public health, as well as access to health and other data, would be under much more local guidance and control, leaving less space for profit and manipulation.

5.3 SURVEILLANCE CAPITALISM

Dataism clearly features strongly in the public health responses to the pandemic and such dataism also characterizes the surveillance capitalism that was at the heart of many pandemic interventions, often to the detriment of the people intended to be served. Dataism has become part of the cultural imaginary (van Dijck 2014) of many contemporary societies, where its dynamics but not its inner workings are commonly understood. By that I mean two things. Firstly, data, hyped by data analysts from the late twentieth century, by tech responses to 9/11, and especially during the pandemic, has a glowing veneer in much of the popular press and media as the source of "solutions" for human crises (Mozorov 2013). Secondly, few in authority, including some data analysts, really claim to understand how algorithms work in practice. Indeed, there is evidence suggesting that the very training of many data analysts is decontextualized. How algorithms might "work in practice" is not necessarily a

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 17:17:18, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009383851.006

central concern to computer science students. At least in North America and Europe, they are often taught in ways that assume "algorithmic objectivity" and "technological autonomy." This kind of thinking tends to privilege technocratic understandings over human experiences of a given phenomenon.

This "disengagement" from the actual human effects and implications of data science is also highly visible in surveillance capitalism, as Shoshana Zuboff (2019) observes. In her hands, it has much to do with what she calls "inevitabilism." This doctrine of inevitabilism, from the "proselytizers of ubiquitous computing" states that what is currently partial will soon become a new phase of history where data science has relieved humanity of much tedious decision-making (Zuboff 2019: 194). Forget human agency and the choices of communities. Just stand by and watch "technologies work their will, resolutely protecting power from challenge" (Zuboff 2019, 224). For Google, one way for this to happen involves Sidewalk Labs, a smart city initiative under the Alphabet (Google's parent company) umbrella. Such cities, one of which almost began life in Toronto, would have had "technology solve big urban problems" and "make a lot of money" (Zuboff 2019, 229). Among other things, Toronto's Sidewalk Labs bid failed because someone asked the questions that Zuboff argues are too often forgotten, "Who knows? Who decides? Who decides who decides?" (Zuboff 2019, 230).

The costs of this disconnection to the human were evident during the pandemic. Much evidence exists of data science disengagement from the questions about how algorithms will be used and of inevitabilism that data science will provide all necessary for a promised recovery and return to "normal." Citizens were often told to simply "listen to the science."[4] Governments wished to be seen as "doing something" and tech companies promised that they could offer systems and software that would address the public health crisis effectively and rapidly.

A case-in-point in Canada is the way that the telecom company Telus sold mobile data to the Public Health Agency of Canada from early stages of the pandemic, something that was not revealed to the public until the end of 2021. This prompted a parliamentary committee to debate the meaning and significance of the move.[5] Various important questions were raised by the federal Office of the Privacy Commissioner. Among them was the reminder that even nominally "deidentified" data still has personal referents and should still be subject to legal protection. Surveillance frequently requires sensitive regulation – and indeed may also need to be dismantled entirely if its results have the potential to threaten human flourishing. In pandemic conditions, inappropriate but avoidable liberties seem to have been taken with commercial data in the hands of a government agency.

[4] Government of Canada records show that "listening to the science" was a key pandemic debate in that country. See www.ourcommons.ca/DocumentViewer/en/44-1/house/sitting-45/hansard.

[5] The ETHI Committee included a speech by the federal Privacy Commissioner, Daniel Therrien, on February 7, 2022. See: www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2022/parl_20220207/

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 17:17:18, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009383851.006

5.4 SURVEILLANCE AS THE "COMMON GAZE"

Here, in summary, are some of the surveillance challenges to human flourishing that were reinforced by the pandemic. Most obvious, perhaps, is the opportunism of tech companies which coincided with the unreadiness of governments for public health crises. This is fertile soil for tech solutionism to flourish in attempts to slow the spread of the COVID-19 virus. Such opportunism builds easily on the dataism that has been establishing itself as a major feature of the twenty-first century zeitgeist in many countries. Dataism, built on older forms of technological utopianism, is myopic and misleading in its approach to data. As José van Dijck (2014) observes, dataism assumes the objectivity of quantification and the potential for tracking human behaviour and sociality from online data. It also presents (meta)data as raw material to be analyzed and processed into predictive algorithms concerning human behaviour (van Dijck 2014, 199).

The problems for ordinary human life arise from the strong likelihood that the conditions for flourishing are not fulfilled when data is granted a superior role in indicating and attempting to ameliorate social problems. As Jacques Ellul (1967) astutely observed (in the 1960s) of the "technological imperative" – it is frequently the case that ends are made to fit the, now digital, means. Today, this critique is updated by Evgeny Mozorov (2013) as "tech solutionism," which had a heyday during the pandemic. As many have observed, pandemic responses frequently misconstrued and failed to address human lived realities.

Today, it is relatively easy to find materials for a radical critique of today's surveillance practices, dependent as they are on varying degrees of dataism and increasingly underpinned by surveillance capitalism. Less straightforward – and perhaps fraught with more risks – is the task of proposing alternatives to the prevailing practices. Not that there is a lack of specific suggestions as to how things might be done differently, from many points of view, but that a coherent *general* sense is missing of "how to go on" that might be agreed upon across such lines. After all, much of the world's population lives in increasingly diverse societies, where finding overarching frameworks for living together is a constant challenge (Taylor 2007).

Human beings require many things in order to truly flourish, not least that they be *recognized* as full persons, with needs and hopes, that are always located in a relational-social context. In a Canadian context, key thinkers such as Charles Taylor and Will Kymlicka have discussed for decades how to develop an inclusive sense of common nationhood in which different groups are *recognized* as playing an equal and appropriate part in the nation.[6] That recognition is vital at several levels but, for both Taylor and Kymlicka, it relates to a sense of basic humanness. Needless to say, their work continues to be debated, importantly, by those, especially from

[6] For example, Charles Taylor (1994a; 1994b) and Will Kymlicka (1989; 1995).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 17:17:18, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009383851.006

feminist and anti-Black racism positions, who consider that their work does not go far enough in recognizing some groups.[7]

This brings me to Eric Stoddart's (2021) work, which focuses on the ways in which surveillance, through its categorizing and sorting – characteristics reinforced by dataism and surveillance capitalism – is socially divisive and militates against both recognition and equal treatment. In particular, such sorting often builds on and extends already existing differences within so-called multicultural societies. Stoddart (2021) concludes *The Common Gaze* with an engaged afterword on some ways that the pandemic experience of surveillance highlights the relevance of his thesis. For instance, he shows how some poorer communities were neglected by healthcare authorities (Stoddart 2021, 221). His alternative human-oriented call is for a "preferential optic for the poor," where those likely to be marginalized receive special attention rather than being abandoned (Stoddart 2021, xiii). Stoddart discusses surveillance as a gaze for the common good; surveillance practiced from a position of compassionate solidarity. Not only this. Such surveillance for the common good would also demand "a preferential *optic* for the poor." From here, Stoddart proposes ways in which data analytics affects certain vulnerable groups more than others and says that the common gaze resists the notion that collateral damage to them is somehow acceptable. Rather, surveillance data, gathered and analyzed differently, could support efforts to shine light on the plight of some specific groups, such as the elderly.

Strikingly, Stoddart does not shrink from considering people as "living human databases" as long as this is not done in a reductionist fashion. Rather, it can be a reminder that we all live as "nodes in complex networks of relationships" (Stoddart 2021, 205). While practices such as self-quantification tend to turn interest inward, the common gaze aims to repair the social fabric, in which solidarity rather than mere connection is at its heart.

Eric Stoddart's *The Common Gaze* (2021) is rooted in socio-theological soil; anyone familiar with liberation theology will recognize the notion of a "preferential option for the poor" as coming from Gustavo Gutiérrez (2001). Stoddart's neat recycling of the term for use in a surveillance context – "a preferential *optic* for the poor" – is a timely reminder of the immense power of surveillance in today's digital world. How we are seen relates directly to how we are represented and treated. Therefore, to question how we *see* becomes truly critical in more than one sense of the word. And it speaks profoundly to how surveillance studies are performed, insofar as that enterprise is intended to contribute to a more truly human world.

Having noted that the common gaze comes from theological soil, it is worth noting that the idea of human flourishing, with which it is closely allied, is a concept

[7] See e.g. Yasmeen Abu-Laban and Christina Gabriel (2008). To hark back to the discussion of pandemic, see Abu-Laban (2021).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 17:17:18, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009383851.006

that actually transcends the barriers sometimes erected – properly, in some senses, to preserve particularity – between different theological positions. As Miroslav Volf (2016) argues in *Flourishing*, the notion of human flourishing is common to many religions, including adherents of the major Abrahamic religions – Jews, Christians, and Muslims. He offers it as a uniting factor, of our common humanity, in a globalized world. If he is correct, and if, beyond that, Stoddart's (2021) work helps us grapple with surveillance in digitized societies, under the banner of a common gaze, then this is a goal worth pursuing. Why? Because it offers hope, at a time when hope seems in short supply.

5.5 A LARGER FRAME

How to turn the question of surveillance, human flourishing, and the common gaze into a matter that can be addressed in relation to the everyday lives of citizens is the challenge. So, what might be said about digital surveillance that connects its practices and discourses with wider debates, ones that are sometimes deemed irrelevant to social scientific or policy-related scholarship?[8] One is that scholars such as José van Dijck (2014) use words such as *belief* in the power of data in data*ism*, indicating an almost "religious" commitment to the findings of data scientists. The other is that the theorist of the "common gaze" writes in an explicitly "religious" context of social theology. Such "larger frames" – though they need not be formally religious in any institutional or theological sense – are necessary to social science and policy studies debates because these disciplines cannot function without making certain assumptions that cannot be "proved" but cannot but be presupposed.

And as soon as terms such as "data justice" and especially "human flourishing" come into play, the discussion is again in the realm of "assumptions" or beliefs about normative matters, about what *should* be. This does not for a moment mean that such analyses are lacking rigour, clarity, consistency, and other expectations rightly held about scholarly work. It simply means that the assumptions about being human, that are all too often obscured by dataism, should be brought into the open, to be scrutinized, criticized, and debated. Of course, if the assumptions can be traced to a "theological" source, this might taint them in the eyes of some who, like Max Weber, consider themselves "religiously unmusical" (Weber 1994, 25). However, Weber was a Lutheran Christian[9] and, while he did not feel qualified to speak "theologically," his work certainly speaks both to sociology and theology.

Here, the notion of "human flourishing" has been mobilized, at least in a rudimentary fashion, to indicate a larger frame for considering questions of digital surveillance in the twenty-first century. The term "human flourishing" is common

[8] See e.g. Lyon et al. (2022).

[9] See e.g. William Swatos and Peter Kivisto (1991) and Joseph Scimecca (2018, 18).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 17:17:18, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009383851.006

to major Abrahamic religions and will thus resonate with large swathes of the global population. And it may be linked, constructively, with terms used here, among various surveillance scholars, such as "data justice." As a goal for refocusing attention on the human in surveillance activities and systems, it deserves serious attention.

REFERENCES

Abu-Laban, Yasmeen. "Multiculturalism: Past Present and Future." *Canadian Diversity* 18, no. 1 (2021): 9–12.

Abu-Laban, Yasmeen, and Christina Gabriel. *Selling Diversity*. Toronto: University of Toronto Press, 2008.

Buolamwini, Joy. *Unmasking AI*. New York: Penguin, 2022.

Chin, Josh, and Liza Lin. *Surveillance State: Inside China's Quest to Launch a New Era of Social Control*. New York: St Martin's Press, 2022.

Cinnamon, Jonathan. "Social Injustice in Surveillance Capitalism." *Surveillance & Society* 15, no. 5 (2017): 609–625.

van Dijck, José. "Datafication, Dataism and Dataveillance: Big Data between Scientific Paradigm and Ideology." *Surveillance & Society* 12, no. 2 (2014): 197–208.

Ellul, Jacques. *The Technological Society*. New York: Vintage, 1967.

Gutiérrez, Gustavo. *A Theology of Liberation*. New York: Orbis, 2001.

Ip, John. "Sunset Clauses and Counter-terrorism Legislation." *Public Law* 27 (February 2013): 1–26. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1853945.

Kitchin, Rob. "Civil Liberties or Public Health, or Civil Liberties and Public Health? Using Surveillance Technologies to Tackle the Spread of COVID-19." *Space & Polity* 24, no. 3 (2020).

Kymlicka, Will. *Liberalism, Community and Culture*. Oxford: Oxford University Press, 1989.
Multicultural Citizenship. Oxford: Oxford University Press, 1995.

Lin, Liza. "China Marshals its Surveillance Powers against Coronavirus." *Wall Street Journal*, February 4, 2020.

Lyon, David. "Reflections on Forty Years of Surveillance Studies." *Surveillance & Society* 20, no. 4 (2022a): 353–356.
ed. *Surveillance as Social Sorting*. London: Routledge, 2003.
"Surveillance, Transparency, and Trust: Critical Challenges from the COVID-19 Pandemic," in *Trust and Transparency in an Age of Surveillance*, edited by Lora Viola and Paweł Laidler. London: Routledge, 2022b.

Lyon, David, et al. *Beyond Big Data Surveillance: Freedom and Fairness*. Kingston: Surveillance Studies Centre, 2022. [The final report of a 6-year research project funded by the SSHRC, led by Kirstie Ball, Colin Bennett, David Lyon, David Murakami Wood, and Valerie Steeves.]

Marquez, Xavier. "Spaces of Appearance and Spaces of Surveillance." *Polity* 44, no. 1 (2012): 6–31.

Mosco, Vincent. *To the Cloud: Big Data in a Turbulent World*. Boulder: Paradigm, 2014.

Mozorov, Evgeny. *To Save Everything, Click Here: The Folly of Technological Solutionism*. New York: Public Affairs, 2013.

Ollier-Malaterre, Ariane. *Living with Digital Surveillance in China: Citizens' Narratives on Technology, Privacy and Governance*. London: Routledge, 2024.

Pei, Minxin. *Sentinel State: Surveillance and the Survival of Dictatorship in China*. Cambridge, MA: Harvard University Press, 2021.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 17:17:18, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009383851.006

Reiman, Jeffrey. "Driving to the Panopticon." *Santa Clara High Technology Law Journal* 11, no. 1 (1995): 27–44. https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1174&context=chtlj.

Scassa, Teresa. "Interesting Amendments to Ontario's Health Data and Private Sector Privacy Laws Buried in Omnibus Bill." *Teresa Scassa* (blog), March 30, 2020. www.teresascassa.ca/index.php?option=com_k2&view=item&id=323:interesting-amendments-to-ontarios-health-data-and-public-sector-privacy-laws-buried-in-omnibus-bill&Itemid=80&tmpl=component&print=1.

Scimecca, Joseph. *Christianity and Sociological Theory*. London: Routledge, 2018.

Stoddart, Eric. *The Common Gaze: Surveillance and the Common Good*. London: SCM, 2021.

Swatos, William, and Peter Kivisto. "Max Weber as 'Christian Sociologist'." *Journal for the Scientific Study of Religion* 30, no. 4 (1991): 347–362.

Taylor, Charles. *Multiculturalism: Examining the Politics of Recognition*. Princeton: Princeton University Press, 1994a.

"The Politics of Recognition" (1992). In *Multiculturalism and "The Politics of Recognition"*, edited by Amy Gutmann. Princeton: Princeton University Press, 1994b.

A Secular Age. Cambridge, MA: Harvard University Press, 2007.

Taylor, Linnet. "The Price of Certainty: How the Politics of Pandemic Data Demand an Ethics of Care." *Big Data & Society* 7, no. 2 (2020): 1.

"What Is Data Justice? The Case for Connecting Digital Rights and Freedoms Globally." *Big Data & Society* 4, no. 2 (2017): 1–14. https://journals.sagepub.com/doi/pdf/10.1177/2053951717736335.

Volf, Miroslav. *Flourishing*. New Haven, CT: Yale University Press, 2016.

Weber, Max. *Max Weber. Briefe. 1909–1910*, edited by M. Rainer Lepsius, Wolfgang J. Mommsen, Birgit Rudhard, and Manfred Schön. Max Weber Gesamtausgabe. II/6. Tübingen: J.C.B. Mohr (Paul Siebeck), 1994.

Xuecun, Murong. *Deadly Quiet City: True Stories from Wuhan*. New York: The New Press, 2023.

Zuboff, Shoshana. *The Age of Surveillance Capitalism*. New York: Public Affairs, 2019.

"Big Other: Surveillance Capitalism and the Prospects of an Information Civilization." *Journal of Information Technology* 30, no. 1 (2015): 75–89.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 17:17:18, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009383851.006

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 17:17:18, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009383851.006