



Body stakes: an existential ethics of care in living with biometrics and AI

Amanda Lagerkvist¹ · Matilda Tudor¹ · Jacek Smolicki³ · Charles M. Ess² · Jenny Eriksson Lundström¹ · Maria Rogg¹

Received: 23 August 2021 / Accepted: 21 March 2022
© The Author(s) 2022

Abstract

This article discusses the key existential stakes of implementing biometrics in human lifeworlds. In this pursuit, we offer a problematization and reinvention of central values often taken for granted within the “ethical turn” of AI development and discourse, such as autonomy, agency, privacy and integrity, as we revisit basic questions about what it means to be human and embodied. Within a framework of existential media studies, we introduce an existential ethics of care—through a conversation between existentialism, virtue ethics, a feminist ethics of care and post-humanist ethics—aiming to deepen and nuance our understanding of the human behind “human-centered” AI directives. The key argument is that biometrics implicates humans through unprecedented forms of objectification, through which the existential body—the relational, intimate and frail human being—is at risk. We interrogate these risks as they become visible at three sites where embodied humans are challenged by biometrics, and thus where the existential body is challenged by the biometric body. This occurs through reductionism (biometric passports nailing bodies to identities, removing human judgment and compromising agency at the AI border), enforced transparency (smart home assistants surveying human intimacies and invading intimate spaces in the bedroom) and the breaching of bodily integrity (chipping bodies to capture sensory data, challenging the very concept of bodily integrity through self-invasive biohacking). Our existential ethics of care is importantly not a solutionist list of principles or suggestions, but a manifesto for a way of thinking about the ethical challenges of living with biometrics in today’s world, by raising the right questions. We argue that a revitalized discussion of the basic existential stakes within human lived experience is needed and should serve as the foundation on which comprehensive frameworks can be built to address the complexities and prospects for ethical machines, responsible biometrics and AI.

Keywords Biometrics · Everyday life · Lifeworld · Bodies · Existential ethics · Ethics of care

✉ Amanda Lagerkvist
amanda.lagerkvist@im.uu.se

Matilda Tudor
matilda.tudor@im.uu.se

Jacek Smolicki
jacek.smolicki@gmail.com

Charles M. Ess
charles.ess@media.uio.no

Jenny Eriksson Lundström
jenny.eriksson@im.uu.se

Maria Rogg
maria.rogg@im.uu.se

¹ Department of Informatics and Media, Uppsala University, Uppsala, Sweden

² Department of Media Studies, University of Oslo, Oslo, Norway

³ Department of Culture and Society (IKOS), Linköping University, Linköping, Sweden

1 Introduction: the right questions beyond the ethical turn¹

In the American science fiction film *I, Robot* (dir. Alex Proyas 2004), the protagonist Del Spooner—an apprehensive and guarded homicide detective (starring Will Smith)—is ambivalently situated in a future of humanoid robots, while being himself dependent on a robotic prosthesis for his own functioning after a trauma. The plot revolves around familiar fantasies and concerns as regards robotic agency and how to control

¹ This article is part of the research project “BioMe: Existential Challenges and Ethical Imperatives of Biometric Artificial Intelligence in Everyday Lifeworlds” headed by Professor Amanda Lagerkvist in the Department of Informatics and Media, Uppsala University, and funded by WASP-HS: <https://wasp-hs.org>.

it and the risks of human over-reliance on potentially raging machines.² All of this is set against horizons of the prospective humanity, sentience and arguable rights of robots. When Dr. Lanning who is a co-founder of the leading corporation in this domain, US Robotics (USR), and its principal scientist, mysteriously dies after falling out of his office window, he leaves behind a message in which he requests that Spooner be assigned to the case. The police declare the death a suicide, but Spooner is suspicious and continues to investigate. In that pursuit, he activates a program in which the hologram of Dr. Lanning is programmed to answer questions. But as Spooner discovers there is a caveat which plainly asserts itself when Lanning states: “My responses are limited. You must ask the right questions.” When the right questions are eventually raised, *nota bene*, the program is terminated. In one key scene Spooner ultimately ventilates his personal concerns about the lack of ethical judgment (or what virtue ethicists call *phronēsis*) in this world of robots, as he tells a USR psychologist about how he got his robot arm. In the aftermath of the car crash, he was saved underwater by a robot (described as a ‘difference engine’) because he had a 45% chance of survival versus a girl named Sarah in another vehicle, aged 12, whose chances were 11% and who was left to die. After describing the robot’s resolution of the trolley problem in his favor, he says: “She was somebody’s baby. 11 percent would have been more than enough. A human being would have known that. Robots, they’ve got nothing here (*gesturing towards his heart*)—nothing but lights and clockwork.” The story thus asks important ethical questions, as it rehearses a well-known framing within which societal and existential values worthy of protection are at risk due to the unholy union of commercial forces hitched to the Faustian ambitions of insatiable engineering minds, seeking, in non-transparent and potentially deeply unethical ways, to achieve complete control over the world via the powers of these new acting technologies.

In the contemporary machine age, by contrast, *everything* seems to be “ethics.” Broad debates on the need for ethical and responsible AI have been running high with regard to risks for (mis)use of technology and personal data, as well as for biased algorithms and designs.³ This has spurred a broad

“ethical turn” involving industry, academia, the public, civil society and policy-makers—and has generated numerous initiatives, guidelines and lists of principles that display similarities in terms of a shared “values canon.” This canon combines utilitarianism with Kantian values, such as privacy and autonomy, and places stress on keywords such as transparency, justice, fairness, minimizing bias, non-maleficence, reducing harm to humans, security, safety, responsibility, accountability, beneficence, trust, sustainability and dignity.⁴ As many have observed though, these values are seldom deliberated at their core, but rather taken for granted. This makes ineffectual “ethics washing” an obvious risk, but even more problematically—and profoundly—ethics is in fact reduced as it emerges as that sought-after *right answer* that solves the issue and ends the problem/program, concluding the exchange. Hence, ethical solutions are all we need, and there is no time for questions without answers! In a world

Footnote 3 (continued)

credit worthiness or, still more seriously, making judgments as to the likelihood of a particular individual committing a crime in so-called pre-emptive policing systems (cf. O’Neill 2016; Hildebrandt 2015) or of recidivism should a prisoner be granted parole (the COMPAS system, Northpointe/equivant.inc), see e.g., Dressel and Farid 18; cf. also Lin et al. 50) – have evoked a range of additional concerns beyond personal integrity. *Contra* promises for social, ecological and economical gains, the threats to human rights and liberties are highlighted due to limited accuracy depending on homogeneous or flawed data (World Economic Forum 68 p. 4). Multiple problems of *bias* (e.g., Gelman, Mattson and Simpson 32; Gates 30; Magnet 54), both in design and the data sets used to train AI systems (O’Neill 2016; Noble 56; Kosinski and Wang 44; Eubanks 24, Crawford 2021) are now well documented. The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems (IEEE 41) thus highlights warnings about among other things, discrimination, adverse economic impacts, risks to security of critical infrastructure, and possible negative long-term effects on societal well-being, thus requesting alignment with society’s defined values and ethical principles, in both legal and technical dimensions.

⁴ This values canon or values monoculture has been identified by aline shakti franzke, after reviewing 85 of these initiatives. The values commonly repeated are further rooted primarily in Kantian deontology – namely, the insistence on protecting basic rights to privacy, equal treatment before the law, freedom of expression, and so on, as grounded in the insistence on the human being as a rational autonomy (Burgess et al. 2018, p. 16; Ess 23, p. 82). So the Ethics Advisory Group (EAG) of the European Data Protection Supervisor (EDPS) emphasizes the “values of dignity, autonomy, freedom, solidarity, equality, democracy and trust” to be foundational to “the European project” – where dignity and autonomy are explicitly linked to “the Kantian idea that human beings are to be understood as ends in themselves and never as a means alone” (ibid). In addition to the GDPR, central EU initiatives and documents frame much contemporary discussion and debate on AI ethics (cf. Floridi et al. 27; Ess 23, p. 82). However, as franzke argues, “While privacy is frequently mentioned, only a handful of guidelines address de facto privacy breaches and the implications of these in the lives of those affected” (e.g., GDPR, or Ethics Guidelines for Trustworthy AI, or The Montreal Declaration for responsible AI development).

² The film is adapted from a screenplay originally suggested by Isaac Asimov in his 1942 short story *Runaround*. The story features the Three Laws of Robotics: 1) A robot may not injure a human being or, through inaction, allow a human being to come to harm. 2) A robot must obey the orders given it by human beings except where such orders would conflict with the First Law. 3) A robot must protect its own existence as long as such protection does not conflict with the First or Second Laws, Asimov, *I Robot*, 1950.

³ In particular, the use of facial recognition technology for vastly diverse areas such as improved consumer experiences or efficient surveillance has been under the ethical microscope, identifying a series of critical risks, such as real time surveillance, privacy infringements by users, unlawful use of private data or data breaches (Harwell and Fowler 35). AI “decision-making” systems – whether for determining

where the future itself has been colonized by AI (Zuboff 69; Lagerkvist 47), ethics is thus formulated in solutionist mode and packaged as actionable principles and tools for assessing how these should be implemented. This includes the idea that design itself should be ethical, trustworthy and value sensitive from the outset. Technology is the prime mover, and ethics is the solutionist remedy.

In this situation, we may ask, why should the humanities bother? With their passion for ambivalence, ambiguity, paradox, the unsettled, the uncertain, the immeasurable, the perverted, the unseen, the hidden, the obscure; with their sensibility for secrets, mysteries, imaginations and complexities; with their sensitivities about limits, embodiment, mortality, and their endless curiosity about our human and also more than human condition, including their critique of normativity—clearly they are off target from the very start. Or is that precisely why they should bother? For within the humanities, raising the ‘right’ or pertinent questions means something entirely different; it is in itself an *ethical practice* which we are in deepest need of in the current moment. Rather than providing or expecting absolute answers or clear-cut ‘solutions,’ asking the right questions about our conduct in digital existence (as the AoIR Ethics 3.0 Guide⁵ also adamantly stresses) is a core value and virtue to cherish. In fact, many of the great traditions in ethics and philosophy—which constitute an essential normative dialog across the centuries about ‘the good life’—have both prevailed without simple answers and can precisely due to this teach us valuable lessons also today. Such a dialog with nuances, respect for otherness and patience—in the spirit of what Charles M. Ess calls ethical pluralism (Ess 20; 21, 22)—is the imperilled core of a democratic society, but also of an existentially sustainable one in which we become human with technologies.

But what then are the ‘right questions’ to ask in relation to ethical AI, at a point in time when everything is defined as ethics and when there are so many initiatives already in place? What can a humanistic and more specifically *existential* approach add to the picture? Apart from sharing in the legitimate concerns about risks that should be taken seriously (Häggström 34), a cue for us can be found in the commonly held idea expressed by the European Commission as well as the High-Level Expert Group on AI in their list of principles for ethically aligned AI that all AI produced in Europe should be “*human-centric*.”⁶ This is key and

should be lingered upon, because, *who is in fact the human behind the expression “human-centered AI”?* As the above-mentioned values canon suggests, when taken for granted, a particular formation of subjectivity is commonly invoked: the famous and famously disavowed ‘liberal humanist subject’—the autonomous, independent, certain economic man who has been critiqued by Foucauldians and feminists for decades. What emerges is thus a masculinist, western subject whose rights, not least to a detached definition of individuality itself, are in need of protection against incursions from machines.

Yet, this is only one highly limited understanding of what it means to be human, in neglect of both human relationality, embodiment and truthful singularity as responsibility; of our conflicted, faulty, and contradictory nature, and of the conditions of deepest uncertainty under which we live today. Such contingencies are heightened as humans are *thrown* into a limit situation of both rapid technological transformations and interrelated crises (Lagerkvist 45, 47, 48). Hence, if we move beyond the above-mentioned version of the liberal subject, we must also ask in this moment: *what do we need to defend if we define humans existentially?* To engage such questions we need to problematize what we actually mean by these commonly agreed upon core values, by returning to the existential grounds upon which all ethical considerations are built. In doing so, our goal here is to define an ethics which identifies not only risks, but also illuminates and takes seriously valued human assets to articulate what is at stake for humans in all their diversity in the face of these massive developments.

One common attempt to move beyond and decenter the liberal humanist subject in contemporary debates on ethics and advanced technologies posits machines as acting as ethical agents, situating ethics transversally across human and more-than-human domains. Conceived to be located both in things, technologies and human subjects, strands of post-humanist discourse see ethics as distributed across various forms of agency (Verbeek 67; Floridi 26; Hayles 36; Dignum 17). While this has profoundly challenged the idea of “human-centered ethics” in highly productive ways, these “cognitive assemblages” as N. Katherine Hayles (36) calls them, simultaneously produce new forms of lived experience. This, we argue, bring humans and their bodies back into the loop, in ways that should evoke a renewed interest in classic existential concerns. In other words, we will not only decenter “the Human,” but we will *re-center humans*, by opening out to a richer and more pluralistic understanding of their traits, needs and qualities. Humans, we argue, should be re-conceived in a multivalent sense, as *coexists* (Lagerkvist 46, 48) who are both differently situated yet sharing in the conditions of deep relationality as embodied, mortal, vulnerable, technological, bereft, situated and ethically responsible beings.

⁵ franzke, aline shakti, Bechmann, Anja, Zimmer, Michael, Ess, Charles and the Association of Internet Researchers (2020). *Internet Research: Ethical Guidelines 3.0*. <https://aoir.org/reports/ethics3.pdf>.

⁶ This is articulated in the coordinated plan for AI made in Europe: http://europa.eu/rapid/press-release_MEMO-18-6690_en.htm, see also https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_draft_ethics_guidelines_18_december.pdf.

More specifically, this article discusses the key existential stakes of implementing biometric AI in human lifeworlds by also offering a rethinking of issues of autonomy, agency, privacy and integrity. It introduces an existential ethics of care—through a conversation between existentialism, virtue ethics, post-humanist ethics and a feminist ethics of care—that sides with and never leaves the vulnerable human body, while recognizing human diversity and the plurality of lived experience of technology. This means accepting the delicate challenge of opening up a normative, yet explorative discussion that after post-humanism reinvents rather than abandons the inviolable human being while resituating her as embedded in the technological environment, thus advancing the emphasis on autonomy to a position of *relational autonomy* (MacKenzie and Stoljar 53). In this vein, and by thus inviting several ethical paradigms seldom in congress into the conversation, we offer much needed and carefully elaborated re-centered human dimensions of the existential stakes of ethical machines and responsible artificial intelligence (AI).

Our key argument is that biometrics implicates humans via unprecedented forms of *objectification*, through which the existential body—the relational, intimate and frail human being—is put at risk. We will interrogate these stakes at three key sites where they are visible and where the existential body is thus challenged by the biometric body. This occurs through *reductionism* (biometric passports nailing bodies to identities and removing human judgment at the AI border), *enforced transparency* (smart home assistants surveying human intimacies and invading obscure spaces in the bedroom) and the *breaching of bodily integrity* (chipping bodies to capture sensory data, challenging the very concept of bodily integrity through self-invasive biohacking). We will further argue that the nailing of bodies to identities through biometrics paradoxically produces a void of embodied existence, hollowing out what it means to be human for humanity “in charge” of the machines, as well as for humanity when exposed to machines. To chisel out our existential ethics of care in this moment, we now turn first to what we consider to be at stake for humans in the present age of biometric artificial intelligence, and then to what must be defended by placing emphasis on some of the incontrovertible aspects, and assets, of being human.

2 What is at stake? Biometrics, ethics and bodies

Biometrics is technology built to measure life, more specifically the digital representations of our unique physiological data and behavior, such as facial patterns, eye retinas, gait, palm geometry and fingerprints, for the purposes of efficient identification and authentication (Ajana 4). In the realm of securitization, law enforcement and the military,

biometrics already has a rather long history, reaching back to the 1960s when efforts were made to teach computers to see and recognize the human face. The automation of identifying human facial expressions was deeply embedded in social and ideological contexts and politically and militarily vested interests (Gates 30). But biometric AI is today also part of our most intimate lives, quantified self-imaginings, embodied perceptions, and our emergent practices of care and of law enforcement through mundane uses of smart watches, home assistants, health applications and contactless border control. Through daily use of information gathering services, we leave behind intimate details about our bodies including health-related data such as fingerprints, heart rates, facial scans and sounds. For example, smart household appliances, so-called digital assistants such as Amazon’s Alexa, Google Assistant and Apple’s Siri, do more than passively follow their users’ voice commands; through new forms of domestic surveillance, corporations record our words and interpret our sounds, often for unspecified purposes. The sum of our embodied data is further increasingly treated as assets for authentication and verification of our “true selves”, and police and judiciary systems are developing both face and voice (dialect) reading, recognition and analysis in preemptive policing and immigration control.

Biometrics is the latest instantiation of what Amanda Lagerkvist has termed “digital thrownness” (45): the sense in which we are thrown into precarious media life, through the combination of fast technological developments; new emergent social norms and habits of digital cultures; the elusive and black-boxed workings of powerful and biased algorithms; and not least through the harvesting of body data within what Shoshana Zuboff calls surveillance capitalism. Lagerkvist stresses that the present moment is in fact a *digital limit situation*, in which there are massive ethico-political stakes for networked humans. By existentializing media, and in proposing a framework for existential media studies, she suggests that we revisit what it means to be human in the present age of techno-cultural saturation. While attending to how existential media both ground us in being and throw us up into the air (implying intensified uncertainties), the approach speaks to our shared embodied vulnerability and deep relationality, and thus demands ethical response—a setting of limits (Lagerkvist 48). In alignment with this stress on limits, an existential ethics of care starts from and never leaves the vulnerable and mortal body—what we coin the *existential body* of “finite and fragile uniqueness” (Cavarero cited in Ajana 3, p. 240)—while also stressing both human responsibility and accountability (Dignum 17). Hence we argue that the ethical challenges raised by these technologies ultimately testify to the fact that even in the age of ever-present machines “*ethics is bodies*” (Thacker 2004, p. 188 in Ajana 4, p. 2, italics added).

What is at stake ethically in biometrically informed lifeworlds, as we have already stressed above, is an all-pervasive form of reinforced objectification of the existential body that *reduces it, forges compulsory transparency* vis-à-vis its resting places and hideouts, and *breaches* it in different and ethically problematic ways. In our case, objectification must however be defined, importantly, beyond disembodied data doubles or “data derivatives” (Amoore 7), since the biometric body is not only “pure information.” Instead, following Btihaj Ajana, objectification produces *recombinant identities* (3) generated by big data which “indicates the actuality of re-individuation, that is to say the terminal point at which data recombine into an identity in the ‘concrete’, ‘corporeal’ and ‘material’. In this context, never, at any stage, could data be considered as ‘purely’ virtual, decorporealised, disembodied or immaterial sense” (Ajana 5, p. 73, cf. Ajana 3, p. 248). Biometrics, as we will argue, is thus *felt in the hurting and sensing body*, as it is implicated by technological intervention.

3 Biometric lifeworlds: three sites

Our argument will be further pursued by moving through three particular sites within our contemporary technologically enforced lifeworld, where we find that something profound is at stake for embodied humans and thus for humanity—in all its plurality—in the machine age. We see those sites as territories of new, technologically saturated limit situations where personal identities are subject to recombination beyond one’s awareness. These sites illustrate where biometrics is now implemented within everyday life, raising crucial ethical questions that all center on tensions between the *existential body* and the *biometric body*. Here, we find bodies in aspiring to movement as to be found by *the border*, bodies in rest and intimacy as to be found in *the bedroom*, and bodies of technological self-invasion incarnated by *the biohacker*.

The sites, spanning both personal and administrative scales, are constellations of practices, decisions, spaces, ideologies and technologies, joined and separated by the mediating body, but there are also existential values to be found at these sites. Therein, we will further illustrate the pressing existential stakes and ethical concerns of these technological interventions for both the prospects of achieving a sense of what virtue ethicists call well-being and flourishing, and of living well together, but also of the inherent threats to these values. By consequence, we also revisit and ‘existentialize’ issues of autonomy, agency, privacy and integrity. Sensing our way across these sites, and making sense of them, by adding different feminist, virtue ethicist and post-humanist acumens to the concoction, we finally arrive at a concluding discussion on care ethics through which the tangs and

traits of our existential ethics of care are intuited and can be articulated. En route to getting there, we offer in the following three imaginative and perhaps provocative scenarios that will serve to flesh out questions, intentionally left unanswered, about how existential needs can be respected in the age of biometrics, so as to also set limits for the pervasive technological architecture of datafication of our time (Zuboff 69). We thus begin by the datafied border.

3.1 The border: reducing human identity to body features and removing human judgment

Imagine yourself standing as an immigration control officer at an airport checkpoint with the long line of travelers in front of you. Your gaze is moving between their warm tired bodies that all look a bit ragged after the long flight, and the screen where their bodily features and accompanying identities are presented one after the other. In the queue, you see business travelers with important faces and well-tailored suits, as well as tourists and those who are probably here to visit their family considering the size of their luggage. Some kids are screaming, holding on to a woman’s skirt, and pearls of sweat are running down from her hijab as she tries to calm them down with her one hand while pressing a sleeping baby toward her chest with the other. On the screen, faces flicker by as the system runs them through, magically revealing their personal data. You think about what to eat. You think about getting home and finally getting some sleep after the long night shift, when the system suddenly raises a warning. It is the woman with all the children facing the camera. She tries to catch your eyes while the children keep on screaming in the background. “Sir, do you want to see my passport? Is there something wrong sir?” But you stay focused on the screen, trying to understand why the system cannot access her records. You look at her passport and the documents she handed you, going through her information including citizenship, traveling history, criminal record, family and associates. Nothing seems quite out of the ordinary. You are tired and you think about your bed. “Can you please take a step back and then face the camera once more?” She immediately follows your command, but the system once again fails to access her records. The baby wakes up and starts moaning. She looks at you in despair while you call for the security officers to come. You know that she will come out of the interrogation room in an hour or so and be allowed to cross the border. You have seen this before. But what can you do? The screen says what it does and your shift is about to end.

The contactless border control is here defined as the use of biometric data-driven, (semi-) automated technologies for the authentication, control and verification of traveler

identities or lie detection.⁷ Based on these systems, contactless border control is being devised and implemented into the lifeworld of individuals, travelers and border officials, throughout the globe. Cumbersome and inexact, the algorithms designed for goal optimization of the border control face the moral uncertainty of the “real world”, situations for which no clear-cut ethical solution exists. Despite recent advances, contemporary artificial systems are in fact insufficient to be pre-programmed for future decisions that simultaneously invoke independent or multi-dimensional ethical judgments (Eckersley 19; Cantwell Smith 12; Zweig 70). Chouliaraki and Georgiou (13) theorize the border as a socio-material assemblage with ramifications on many legal and political levels pertaining to nations and institutions, but also existentially to personhood and identity of self. With this backdrop, contactless border controls invoke a set of ethical debates that center on the increasing solidification of connections between the body and identity, technology and biology (Ajana 4, p. 88f). Via algorithms, the biometrical data of the body anchors a person’s identity and the individual is thrown into the role as mediator, while becoming itself the point of separation. But in a stroke, body and identity are separated in case of a failure or shortcoming of the technology. In other words: Who are you when the connection to the biometric databases fail? As the databases and systems increasingly transcend national and state borders, the accountability of data is weakened and dispersed, while its recognized flaws and biases that often target marginalized groups (Eubanks 24) continue to reinforce bias of race and gender (Browne 11). What institution can validate identity, when the body itself fails to do so?

The seeming disappearance of borders (Amoore 6) as we know them further entails the emergence of new kinds of borders even if they are imperceptible to our human sensorium. Disappearance of a human-operated border control infrastructure entails the emergence of not only computing infrastructure, network devices and software, but also of altered human relations and orientations in time and space. Taking the existential body as the point of departure invokes a wholly different form of autonomy

indebted to our deep relationality, since it reminds us of the ways in which human responsibility and accountability are reliant upon our inherent openness to one another. Ethics then, following Levinas (49 [1979]), is a potential for truly facing the other, since the face signifies an order of responsibility—a moral obligation. The face, now reduced to standardized points of measurement, is in fact what cannot be controlled and constitutes the very exteriority of the other which makes her stand out in the world of objects. In that sense, the biometric border deprives us of the relationality of being which is constituted as Merleau-Ponty argues by this bodily reciprocity which opens us out to one another, and thereby situates “the other as an essential structure of being human” (Merleau-Ponty 55, 483). Hence, our deep relationality as existential beings—our *self-constitution through others in communication* (Jaspers 42/1970, 64)—is compromised by biometric passports, and other forms of automated decision making. Hence, this co-existential form of selfhood has nothing to do with the construction of an *identity* via the comparison to a datafied double that is created in relation to vast databases on thousands of others. By their instrumental de-humanized control mechanisms these machines furthermore contribute to increasingly distancing us from the active negotiation that relationality calls upon us. In biometric and algorithmic cultures, relationality—one’s potential and need to establish relations—is pre-programmed, imposed and stifled. In a complex and messy world where we are constantly striving for greater efficiency, borders are losing touch with human reflective judgment while the flows of bodies across distances are increasingly talked about in terms of faceless volumes. This touches right at the heart of Shannon Vallors’s 12 techno-moral virtues where human *phronēsis* is center stage, i.e., the “practical wisdom” that should be the central capacity for judging an ethically informed response within specific concrete, fine-grained circumstances that are otherwise intractable for more deterministic, “rule-book” approaches such as deontology and utilitarianism.⁸ In a move resonant with this emphasis, Mark Coeckelbergh also recently advances this approach in interesting ways, beyond individual agency, by integrating relationality, embodiment and practice into the very definition of virtues vis-à-vis AI ethics (15, 16).

⁷ As Pfeifer (61) has comprehensively discussed, in the EU, eu-LISA agency manages several large-scale IT systems such as the Schengen Information System (SISII), the Visa information System (VIS), the Entry/Exit System and the European travel information authorization system (ETIAS) and the European Criminal Records Information System—Third-Country Nationals (ECRIS-TCN), all for the purpose to improve access to information stored in the information systems and identity management at the EU level (European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice, 2021). In the US the Integrated Case Management (ICM) provides us with another example of integrated biometric databases built for facilitating border control (U.S. Department of Homeland Security 2016).

⁸ However, it needs to be stressed that opening up the contactless borders for existential intervention does not in any way imply a naïve nostalgia for borders guarded by human judgment. Instead it urges us to reflect critically on the practices of *bordering* (Keshavarz 43) at large as always and already techniques of determining, shaping, and even disabling coexistence. However, contactless borders on the other hand, certainly do not in any simple way advance ethical and political concerns ingrained in these practices.

Seeing the border as an ethically charged zone of coexistence urgently calling for negotiation, what automated decision-making seems to do, is to evacuate human responsibility and potentially also autonomy and agency. Even if commonly flawed and biased, at the very least, the existence of the border guard as an embodied subject in charge, did promise a possibility to enter a zone of dialog (or even a dialogical confrontation) as opposed to a zone of passive, preemptively non-negotiable verification of one's status, based on a reduced set of body features. The right questions to ask then seem to be: what are the prospects for human dignity and respectful coexistence in a world where we are habituating such an instrumental gaze at the other, and where complicated and imperfect decisions-making processes are left to machines? What will be the fate of human autonomy and judgment as gut feeling in decision making, when identity, rights and responsibilities are solely based on a reduced set of body features rendered as data?

3.2 The bedroom: the transparent body and the perversion and plainness of everyday living

Imagine yourself returning home after an exhausting day at work. After dinner and chores, you and your partner enter the bedroom which comes about as a warm, soft cave in the evening dusk; a uterus made of down for you to withdraw and rest your weary head and bodies. You lie down on top of the bed, facing each other and begin a conversation about goings-on at work. You have dimmed your lights and set your phone on silent. You feel increasingly detached from the external world and more present here and now. As you ask your smart home assistant to put on some background music, the device fulfills your wish in a matter of an instance. Your wish is its command. Yet, as you turn to your partner to ask a question, the machine suddenly responds in your partner's place. This throws you out of joint. The device's instant readiness reminds you that it is passively listening to your conversation, and of course everything else that goes on in the bedroom. You think of how desensitized your alertness has become to this presence of an alien element in your most intimate space. Who is actually commanding whom in this relationship? There and then, the devices that surround you, to make you feel independent and calm, make you feel uneasy. That night you fail to fall asleep. A few days later, you start receiving targeted advertisements about insomnia treatment in your social media feed.

As smart home assistants are quickly becoming the fastest growing device category around the globe, we are predicted to face a new human-machine paradigm dominated by voice interaction rather than text in- and output. In 2018 alone,

100 million Alexa devices were sold globally.⁹ According to Ovum, in 2021 there might be almost as many voice-activated smart assistants on the planet as people.¹⁰ As organizing infrastructure for our ever-smarter living spaces, the home assistants raise issues about corporate invasion creeping deeper and deeper into our personal lives. How can the existential body be safeguarded in this situation? Here, we thus use the site of the bedroom in order to highlight issues associated with intimate personhood. First, the bedroom is indicative of that which we usually think about as our most "private" lives commonly connected (but in no ways limited) to the sphere of the home. In Shoshana Zuboff's (69) analysis of the datafication of human experience for corporate interests, she describes the endless surge for new raw material for the production of ever more precise prediction products. This process is driven by an increasing awareness of the value of behavioral surplus and propels a development where artifacts and services pose as one thing, such as a smart assistant, a baby watcher, a thermostat and so on, but are in fact primarily targeting the peripheral surplus: our temperament, habits, social relations, background noise, etc. Importantly, this is being done to a very high extent without people being consciously aware of being under constant surveillance within their private homes, while they are conversing over dinner, arguing with their partner, speaking to themselves, singing in the shower, making love. While we are being taught by imperatives on transparency that we have nothing to fear if we have nothing to hide (such as spelled out by Google's former CEO Eric Schmidt), we mean that fundamental aspects of being human are forgotten.

The bedroom perhaps more than any other space highlights the essential need and right to be able to retreat to spaces for rest, pleasure and unproductivity, spaces to let down our guard. Ultimately, this may be symbolized by the immense vulnerability of the sleeping body in all its inattentive trustfulness. At the same time, the bedroom must not be conflated with "the home" in any simplistic, literal sense but implies a sense of privacy that often bleeds between locations, in which existential security can both be lost and had. From queer communities, we can learn that such personal spheres can be constituted by an intermingling of what is traditionally understood as private, public, pleasure and politics (e.g., Berlant and Warner 10). Nowadays for example, same-sex dating applications are often considered highly intimate spaces among non-heterosexual communities, and the 2018 scandal where the predominantly gay male app Grindr sold highly sensitive information, for example about their users' HIV status, to third parties, provides an illustrative example

⁹ <https://policyadvice.net/insurance/insights/amazon-alexa-statistics/>.

¹⁰ <https://www.theatlantic.com/magazine/archive/2018/11/alexa-how-will-you-change-us/570844/>.

of how such intimate information can be exploited. This means that demands on privacy protection must take its starting points from an understanding of a multi-faceted and multi-sited human being rather than from specific designated spaces such as the ‘family home’ where particular individuals are envisioned to be located.¹¹ It could be argued that the bedroom presents us with the perversion of everyday living, as a necessary aspect of existence and a take on privacy that goes beyond the liberal subject and his need for autonomy. Such privacy, we importantly argue, includes *the right to opacity* for that overflow of human activity which transgresses, is inconsistent, dishonourable and thus needs to escape the terror of transparency and accountability. Human beings should have the right to not only privacy in any libertarian sense, but to secrecy, dubiousness, and hidden closets—intimate spheres of our own where we may trial and error and let down our guard, often connected to bodily pleasures and needs. We also have the right to be plain and invisible in laying claims to nothing. This is not the same as saying that these values should be kept away from the public, but that they should be regarded as highly vulnerable assets of the singular human being, signalling limits for the data gathering industry. As such, the bedroom highlights that intimacy must be based on consensual relations and reminding of the demands from feminist data ethics (Cifor et al. 14), of committing to a type of data regime that knits the “no” into its fabric. Further, it is important to remember that surveillance works in discursive ways, fostering discipline on behalf of the body subject (Foucault, 1977). So if it is true as the psychoanalytical tradition would tell us, that our lives contain both conscious, secret and unconscious dimensions, the right existential question to ask is perhaps: what happens to us when all these dimensions are treated as equally available for data extraction and objectification? As we are constantly thrown back at ourselves by algorithmic reflection, will the subject become ever more transparent to herself, illuminated into every dark corner? Then, will the disciplining terror of complete transparency haunt every single bit of human life?

As we have now covered biometric objectification of the relational other, of selves in charge via machines at the airport, and of the existential body in the bedroom, we will at

the last site turn to the objectification of the organic body by biohackers.

3.3 The biohacker: the breached body and the ephemerality of subjectivity

Imagine yourself having been invited to an event by a friend who is a self-proclaimed biohacker. It is a Friday night after-work mingle at a central address in the city, and no costs have been spared. You and your friend have just had a vivid discussion about what on earth makes her voluntarily transplant digital gadgets into her body and she has explained that to her, being in full charge even of the risks, is a journey of (self-)discovery. You are already on your second glass of champagne when a young, handsome man asks for everyone’s attention and presents himself as the company leader and initiator of the local microchipping movement. Your friend seems excited and the atmosphere is vibrating as the man exclaims that you who are there tonight are at the very forefront of a revolution. You are already ahead of the future; a future where the boundaries between man and machine will no longer be meaningful, as we have reached the end of evolution. Humans have no natural enemies left. Everything that follows from now on is artificial. Denying it means nothing but stagnation. Your friend has told you earlier that before the night is over, every visitor will be offered to have a microchip implanted in their arm that will enable seamless purchases and identification. Before coming here you felt fairly skeptical about the whole idea, but now being here with the enthusiastic crowd and the inspirational talk, you find it difficult to remember what your skepticism was about. So when the line to the chipping booths starts to fill up you join your friend. A few weeks later, you have already become accustomed to scanning your wrist as payment method when the morning news reports about a big privacy breach scandal. Apparently, a local tech company has implanted microchips with unspecified software which has been used to extract data to be sold for third parties connected to the right-wing Populist Party on the rise.

In a culture replete with measurement and ubiquitous networks, humans have turned to self-quantification and self-invasion practices, as a means for both utility and social and individual transformation (Lupton 2017; Ajana 2018; Fors et al. 28). By exploring the continuous becoming of the human body as a techno-cultural practice, the community of body hackers go further by deconstructing the idea of an unchanging core of personhood. As an active negotiation between technology and biology, new and fluid subjectivities emerge whose amplified irises, sensor-armed fingertips or wrinkle freed skin (Hines 39; House 40) expose biometrics’ banal defect: the failure to read other bodies, bodies outside the norm. Identifying them would require humane hallmarks—situational, empathetic, and imaginative qualities

¹¹ Helen Nissenbaum (2010) similarly offers the concept of “contextual integrity” for this type of specification in her famous redefinition of privacy away from specified bits/kinds of information to information that is shared within specific relationships and webs of relationships. H. Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press: Palo Alto, CA 2010. For discussion, see Zimmer (2018). Michael Zimmer (2018) Addressing Conceptual Gaps in Big Data Research Ethics: An Application of Contextual Integrity. *Social Media + Society*, April-June 2018: 1–11. <https://doi.org/10.1177/20563051187683>.

that our machines lack. Yet, from an existential point of view, it is here, in the fluid domain of selfhood, where “the ethical plane unfolds” (Ajana 4, p. 87). Since learning to become human with machines informs our ethical agency in and around them, biohacking may constitute both guidance and risk for an existentialist ethics of care.

Today, biometrics govern “the body as a constant entity that can be compared to other entities outside time variants” (Ajana 4, p. 86). Treated as a fixed substance, the body gets boxed and organized according to its attributes (sex, age, class and skin tone), aiming to establish a 1:1 correspondence between the individual and data abstractions of her live body. That way biometric identification installs a reidentification of the same (Gallagher 2017, p. 31). The fixed body and its description are the object, mechanism but also as biohackers expose, the blindside of biometric life and identity politics. At the same time, we need to ask: is the act to chip oneself *only* an act of transgression and rebellion? Or is the potential ethical problem in fact located on a different level? Ajana holds that “the function creep of biometric identity systems can be addressed in light of their spillover from exceptional spaces [...] to the general body of humanity in terms of their becoming a normative and all-encompassing practice” (4, p. 6). Perhaps then, in the end, the biggest ethical concern pertains to such questions about new enforced normativities—the chipped body as the new normal?—and new ensuing vulnerabilities. In other words, an existential ethics of care needs to take into account that the way we compose our lives with technologies today—that is our current forms of engagements with technologies (along with the attempts to reconfigure their dynamics)—are not only determined by factors, processes, biases and inequalities of the past (e.g., Benjamin 9) but will have a ripple effect in the future. Rethinking the ethics of technology in this light might help us better understand, inspect and tangibly identify our entwinement in complex, often problematic relationships that span histories, places and agencies. To date, self-invasive biohacking practices are foremost phenomena occurring among elites of tech-savvy, intellectual and/or artistic groups where the hacking of bodies is largely done in the name of both individual autonomy and within a more progressive narrative, with the aims to provide protection against racism, sexism, and ableism, that is, protection of marginalized groups. It is however not far-fetched to imagine that if the use of technological artifacts inside the human body would move from the exceptional domain of art experiments and life-saving surgery (e.g., pacemakers) to the mundane area of consumer practices and policy monitoring, those who are most likely to be targeted are less advantaged groups. Already today there is numerous evidence of the ways in which the previously unexploited resource of personal and physiological body data captured by biometric AI are currently feeding into systems of

oppression and injustice, disproportionately targeting racialized poor and queer minorities (cf. Eubanks 24; Benjamin, 9). It is perhaps not very hard to imagine that people seeking asylum in Europe—who already have had to find themselves in a situation where their body data is captured and stored in enormous data bases as resources to restrict and control their movement across the continent—would need to accept a microchip in exchange for entrance. Marginalized groups would in a similar manner be the most vulnerable to a consumer culture where participation becomes conditioned on allowing surveillance capitalism even closer onto/into our bodies. As smoother payment practices, VR experiences and well-tailored dating services will be promised, all that is needed is constant access to your heart beat, bloodstreams and optic nerve. The right question is perhaps: should the body—here breached by listening, counting and calculating gadgets—in fact, as Lagerkvist has argued in her media theory of limits and limit situations (48)—in itself constitute an absolute limit against these phenomena? In aiming for an existential ethics of care, the right question to ask in terms of this site might also be to what extent technological solutionism is building us into systems made for a sunny day? That is, systems based on the prerequisite of democratic, friendly forces endlessly aiming to enhance our lives. This is of course already today very far from reality, and variously so, depending on where you happen to live on the planet. But we believe that we are yet to see what kinds of all-out abuse that could emerge through the implementation of these mass surveillance systems in our imperfect, fragile world.

3.4 Summing up the sites and inviting care

Biometrics, as we have shown in this section, challenges the existential body through heightened and unprecedented forms of *objectification* of the body, in the shape of biometric bodies of datafication that always remain material and concrete. At the border it is challenged by the *reductionist body*, which through biometric passports and contact less border controls enable some to project themselves in space and time, while others are deemed as risk subjects without movement. As we have argued, this form of objectification as reduction also implies a severing of the identified individual from both the singular person, and the existential body from her relational being. As previously stated, the unique historical person—the existential body—always in becoming as Kierkegaard classically argued in *The Sickness unto Death*—is now in risk of being redacted into mere parameterized snapshots of personhood, based on not only fixed datafications of the individual itself, but the fixed datafication of thousands of others, equally reduced (Lury and Day 52). This nailing of bodies to quantified, objectified identities, produces paradoxically an evacuation of the fullness of the existential body, hollowing out what it means

to be human. In fact, an equally problematic reduction and sequestration also occurs, as we discussed above, as officers at the border are bound to the machine, and have to downplay their own judgment, and deafen themselves to any narratives that the traveler wishes to communicate.¹² In other words, the situation diminishes and subdues our inherent relational autonomy.

As we saw in the bedroom, the existential body was further threatened by the prospects of *the transparent body*, which is a biometrically forged body without secrets and whose existential needs for obscurity, alterity, queerness but also sleep and rest are invaded by the surveillance technologies of smart home assistants. Finally, in the biohacker we found a *breached body*, where bodily integrity itself was further called into question, by the self-invasive practices of chipping. The existential body in both irreducibility, secrecy and within limits, is challenged through this ephemeral recombinant identity, an externalized self in becoming, re-affirmed through numbers and self-quantification and always transparently available and never at peace in non-accountable obscurity.

All of this leads us to conclude that *care* must be built in as a core principle for biometric AI development. Care, drawing on landmark works in feminist ethics of care, implies an ethics that is less depending on abstract principles and more on the ability to put oneself in the shoes of the other (Noddings 57; Ruddick 63; Held 37). While androcentric ethics would put the autonomous individual at the center, a feminist ethics of care characteristically starts from a human being radically *dependent* on others and its environment. Closely resembling virtue ethics, care can be seen as an ethical core principle (among others) for a responsible human coexistence in face of shared vulnerability (c.f. Held 37; Tronto 64), but also with a pluralist consciousness that reflexively starts from those most likely to be exposed in any given situation. This form of ethics of care is in close alignment with the goals of existential media studies and its practices of slowing down in careful attendance (Lagerkvist 48). As Fisher and Tronto emphasize in their classic definition of care:

[W]e suggest that caring be viewed a species activity that includes everything that we do to maintain, continue, and repair our “world” so that we can live in it as well as possible. That world includes our bodies, our selves, and our environment, all of which we seek to interweave in a complex, life-sustaining web (Tronto 64, 103).

¹² As Ajana similarly concludes: “paradoxically, in its pursuit of capturing the singularity of the person, biometrics only ends up by obstructing the exposure of singularity precisely because of its amputation of narrative from the sphere of identity” (2010, p. 252).

Building on such discussions, our existential ethics of care also wishes to expand on the traditional understanding of the existential as inclusive of, but also beyond the singularity of the human body, to emphasize first in line with Jaspers’ philosophy, the *intersubjective dimension* and then also *intergenerational entanglements* with history and the future (as already suggested above), and the responsibilities also before other than human realms (Puig de la Bellacasa 62). Hence, we also aim to broaden the existential purview by inviting crucial strands of post-humanist ethics into our project (Zylinska 71). If historically, ethical considerations used to pertain to the human condition alone (with a priority given to the condition of a white, western European man), today they need to encompass agencies and realms that stretch far beyond that perspective. Diverse forms of coexistence that we individuals and societies compose with technologies are becoming ever more integrally invested in multiple other realms “out there” of both human and more than human nature. Moreover, those multiple other realms have their extensions in time. This move might help us better understand, inspect and more tangibly identify our entwinement in complex and often problematic relationships that span history, places and agencies. What this means is that we urgently need to recalibrate our ethical incentives and sensitivities so they encompass perspectives on, on the one hand, certain yet often unacknowledged past(s) and, on the other, uncertain future(s). We need to learn how to ethically navigate—conceptually and practically, philosophically and creatively—through those realms and temporalities.¹³ A trivial or enforced decision to improve our life, or some aspect of it, by deploying what is presented to us in terms of a technological solution or remedy (be it a smart speaker, a biometric pass port or chip implant etc.) has its forward reaching material implications as well as backward stretching roots. In other words, our interactions with technologies establish complex relational ecologies characterized by temporal, spatial and multi-agential structures and relations. In sum, this implies an understanding that thoroughly historicizes humans, embeds them in webs of caretaking, while placing ethical responsibility in the present, on a horizon of anticipation and care (Adam and Groves 1; Groves 33).

¹³ Or as Plato put it: “An outstanding pilot [*cybernetes*] or doctor is aware [literally: feels her way through] of the difference between what is impossible in her art and what is possible, and she attempts the one, and lets the other go; and if, after all, she should still trip up in any way, she is competent to set himself aright” (*Republic*, 360e–361a). The *cybernetes* is thus the exemplar of *phronēsis* as both practical wisdom and reflective judgment, and “navigation” a key metaphor and analogy of how we seek to manoeuvre through often unknown, potentially perilous territories and situations. Cf. Peters (60).

4 A manifesto for an existential ethics of care

As we stressed from the onset, the way in which the conditions for debates on AI and ethics is set often makes the humanities disqualified from the start, despite the fact that ethics has for thousands of years constituted one of their core proficiencies. Through our deliberations we hope to have discounted such disrepute. In safeguarding the human defined as the existential body, situating it in relation to biometric technology—and in mapping some of the existential stakes and ethical concerns that biometrics raises within our contemporary lifeworlds—we also believe that we have in this article begun to ask the right questions.

We have argued through three scenarios that biometrics presents us with lived experiences amounting to massive forms of objectification of body, self and identity. This requires something new of us also as scholars. In the vein of Ajana, who calls for new ways of ‘performing’ research, we need approaches that “blur the boundaries between the creative/ experimental and the scholarly/academic [...] that can implant the researcher straight at the heart of the burning socio-political and ethical issues in a radically embodied and affective way” (Beer 8, p. 331). One such approach is an existential ethics of care which will allow for the critical balancing, on the rim, between stressing potentially beneficial and yet irreducibly burdensome dimensions of biometrics—simultaneously (cf. Lagerkvist ed. 46, 48). An existential ethics of care implies in the first instance a conscious move back toward more fundamental questions of existential nature. We argue that we need to begin by revisiting core existential and humanistic questions as the foundation for thinking ethically about biometrics and responsible AI so as to expand on them, such as; what/who is human? What is a human body? How can we safeguard identified existential needs and necessities and human assets and values, in an age of increased automation? We suggest that such existentially informed questions (regardless whether they are answered or remain intentionally open) should become a basis for a *diversified ethical approach*. Heeding a plurality of ethical views is one prerequisite for arriving at responsible AI, or responsible technology at large. Hence, as we have seen, an existential ethics of care implies an interaction of multiple ethical traditions, beyond the current ethical turn—encounters that may both be beneficiary and entail friction, but foremost bring forward the human and her complex relations to identity and body. However, we hold that friction and difference in views can also be productive (Ess 21). Again, our intention is not to lean toward reconciliation of those views. Rather, by foregrounding the existential dimension of our inseparably entangled human coexistence with technologies, we hope to create a more solid ground for exploring

how those views can productively speak to each other. One key merit of this proposed existential ethics of care is thus its insistence on productive and careful collisions as a virtue in itself in a complex technological era. Importantly our existential ethics of care also recognizes that caring stretches beyond our own historical and technological moment. While often tightly, yet imperceptibly tied to environmental, social and racial forms of exploitation established in the past, these ecologies that we voluntarily or involuntarily compose, partake in, reconfigure or are, again, being persistently thrown into, subsequently form sediments for techno-realities (and techno-agencies) to come. An ethics of care thus also pertains to at/tending to one’s awareness of the faint layers, extensions and implications of technologies often operating beyond the scope of one’s individual life and yet with direct material implications on its currents (see Adam and Groves 1).

Our existential ethics of care is importantly not a solutionist list of principles or suggestions, but a manifesto for a way of thinking about the ethical challenges of living with biometrics in today’s world. Hence, our intention here is not to contribute with another program for responsible AI, but instead to open up for a critical reflection about what it means to be human in the age of AI hype and inevitabilism. We have shown that the unprecedented increase of automated technologies rapidly brought into human lifeworlds unavoidably imposes new forms of orientations and disorientations, rearranging scales, coordinates and codes of conduct as we navigate through everyday life. But disorientation does not by any means entail a necessity for re-orientation (c.f. Ahmed 2) or a radical counter-move (*de*-orientation, if you will). Rather, this condition may as well be regarded an opportunity to stay with the friction, with renewed attention to these basic questions about the human existent, refusing any tech-solutionist impulse to straighten out the lines with the only goal to ‘terminate the program.’

Finally, we must stress that even in its most coherent form the existential ethics of care includes modes of questioning, rewiring and opening up ethical assumptions, rather than providing fixed tools or frameworks for solving ethical dilemmas. We believe that the focus on these existential dimensions and ethical concerns within human lived experience might be beneficial for not just one type of audience or one kind of expertise. Our intention instead is to inform relations that emerge in/through transdisciplinary collaboration on responsible and meaningful technologies. Hence, in this essay we hope to have provided an agenda that illustrates the virtues of the existential approach to biometric technologies mobilized in conversation with other traditions by shedding existential light on those relations, connections, threads and links between various perspectives (or shedding light on the lack thereof). While our contested techno-cultural condition might be indeed calling for a widely spanning

ethical approach (and for guidelines etc.), we have shown that this however also encompasses insights on a smaller scale, emanating from particular sites within our lifeworlds where our lives are played out. These may in turn serve as the foundation on which comprehensive frameworks—but also everyday interaction in human as well as more than human domains—can be built to address the complexities and prospects for ethical and responsible biometrics and AI.

Author contributions This article has been a joint venture between all contributing authors, but the order of the authors reflects their level of contribution.

Funding Open access funding provided by Uppsala University. The research has been enabled by a grant from The Marianne and Marcus Wallenberg Foundation (Grant MMW2019.0012) and is part of the project “BioMe: Existential Challenges and Ethical Imperatives of Biometric AI in Everyday Lifeworlds” within the WASP-HS program: <https://wasp-hs.org>.

Availability of data and material Not applicable.

Code availability Not applicable.

Declarations

Conflict of interest The authors declare that they have no conflict of interest.

Ethical approval The BioMe project has been approved by the Swedish National Authority for Ethics Approvals (2020-04982).

Consent to participate Not applicable.

Consent for publication Not applicable.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

References

- Adam B, Groves C (2011) Futures tended: care and future oriented responsibility. *Bull Sci Technol Soc* 31(1):17–27. <https://doi.org/10.1177/0270467610391237>
- Ahmed S (2006) *Queer phenomenology. Orientations, objects, others*. Duke University Press, Durham
- Ajana B (2010) Recombinant identities: biometrics and narrative bioethics. *Bioethical Inquiry* 7:237–258. <https://doi.org/10.1007/s11673-010-9228-4>
- Ajana B (2013) *Governing through biometrics The biopolitics of identity*. Palgrave Macmillan, London. <https://doi.org/10.1057/9781137290755>
- Ajana B (2015) Augmented borders: big data and the ethics of immigration control. *JICES* 13(1):58–78. <https://doi.org/10.1108/JICES-01-2014-0005>
- Amoore L (2006) Biometric borders: governing mobilities in the war on terror. *Polit Geogr* 25:336–351. <https://doi.org/10.1016/j.polgeo.2006.02.001>
- Amoore L (2011) Data derivatives: on the emergence of a security risk calculus for our times. *Theory Cult Soc* 28(6):24–43. <https://doi.org/10.1177/0263276411417430>
- Beer D (2014) The biopolitics of biometrics. An interview with Btihaj Ajana. *Theory Cult Soc* 31(7/8):330–336. <https://doi.org/10.1177/0263276414546380>
- Benjamin R (2019) *Race after technology. Abolitionist tools for the new Jim Code*. Polity Press, Cambridge. www.kvab.be/sites/default/rest/blobs/1501/tw_privacy_en.pdf
- Berlant L, Warner M (1998) Sex in public. *Crit Inq* 24(2):547–566
- Browne S (2015) Dark matters: on the surveillance of blackness. In: Duke UP, Durham Burgess J, Floridi, P, Pols, L, van den Hoven A, eds (2018) *EDPS Ethics advisory group. Report 2018. 18–01–25_eag_report_en.pdf* (europa.eu)
- Cantwell Smith B (2019) *The promise of artificial intelligence: reckoning and judgment*. MIT Press, Cambridge
- Chouliaraki L, Georgiou M (2019) The digital border: mobility beyond territorial and symbolic divides. *Eur J Commun* 34(6):594–605. <https://doi.org/10.1177/0267323119886147>
- Cifor M, Garcia P, Cowan, TL, Rault J, Sutherland T, Chan A, Rode J, Hoffmann AL, Saleh N, Nakamura L (2019) *Feminist data manifest-No.* <https://www.manifestno.com/>. Accessed 13 Mar 2020
- Coeckelbergh M (2020) *AI ethics*. MIT Press, London
- Coeckelbergh M (2021) How to use virtue ethics for thinking about the moral standing of social robots: a relational interpretation in terms of practices, habits, and performance. *Int J Soc Robot* 13:31–40. <https://doi.org/10.1007/s12369-020-00707-z>
- Dignum V (2019) *Responsible artificial intelligence: how to develop and use AI in a responsible way*. Springer
- Dressel J, Farid H (2018) The accuracy, fairness, and limits of predicting recidivism. *Sci Adv*. <https://doi.org/10.1126/sciadv.aao5580>
- Eckersley P (2018) Impossibility and uncertainty theorems in AI value alignment (or why your AGI should not have a utility function). Cornell University. [arXiv:1901.00064](https://arxiv.org/abs/1901.00064) [cs.AI]
- Ess C (2020a) *Digital media ethics, 3rd edn*. Polity, Cambridge
- Ess C (2020b) Interpretative pros hen pluralism: from computer-mediated colonization to a pluralistic intercultural digital ethics. *Philos Technol*. <https://doi.org/10.1007/s13347-020-00412-9>
- Ess C (2020c) Towards an existential and emancipatory ethic of technology. In: Vallor S (ed) *Oxford handbook of philosophy and technology*. OUP, Cambridge
- Ess C (2019) Intercultural privacy: a Nordic perspective. In: Behrendt J, Loh W, Matzner T, Misselhorn C (eds) *Privatsphäre 4.0. Eine Neuverortung des Privaten im Zeitalter der Digitalisierung*, pp 73–88. J.B. Metzler.
- Eubanks V (2018) *Automating inequality: how high-tech tools profile, police, and punish the poor*. St. Martin's Press, New York
- European Union Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (2021) eu-LISA. <https://www.eulisa.europa.eu>. Accessed 22 Feb 2021
- Floridi L (2016) Faultless responsibility: on the nature and allocation of moral responsibility for distributed moral actions. *Philos Trans* 374(2083):20160112

- Floridi L, Cowl J, Beltrametti M, Chatila R, Chazerand P, Dignum V, Luetge C, Madelin R, Pagallo U, Rossi F, Schafer B, Valcke P, Vayena E (2018) An ethical framework for a good AI society: opportunities, risks, principles, and recommendations. *Mind Mach* 28:689–707. <https://doi.org/10.1007/s11023-018-9482-5>
- Fors V, Pink S, Odell T (eds) (2020) *The imagining of personal data: experiences of self-tracking*. Taylor & Francis Group
- Franzke AS (2020) An explorative qualitative analysis of AI ethics guidelines. Unpublished MS Gallagher R (2017) *Videogames, identity and digital subjectivity*. Routledge, New York
- Gates K (2011) *Our biometric future*. New York University Press, New York
- Gallagher R (2017) *Videogames, identity and digital subjectivity*. Routledge, New York, London
- GDPR (2018) General data protection regulation (GDPR) Official legal text. <https://gdpr-info.eu/>. Accessed 3 Mar 2021
- Gelman A, Mattson G, Simpson D (2018) Gaydar and the fallacy of decontextualized measurement. *Sociol Sci* 5:270–280. <https://doi.org/10.15195/v5.a12>
- Groves C (2021) Flourishing for the future: anticipation as meta-capability. In: Spiers E, Lopez-Galviz C, Spiers E (eds) *Routledge handbook of social futures*. Routledge, London
- Häggström O (2021) *Tänkande maskiner. Den artificiella intelligensens genombrott. Fri tanke*, Stockholm
- Harwell D, Fowler GA (2019) U.S. customs and border protection says photos of travellers were taken in a data breach. *The Washington Post*. <https://www.washingtonpost.com/technology/2019/06/10/us-customs-border-protection-says-photos-travelers-into-out-count-ry-were-recently-taken-data-breach/>. Accessed 15 Mar 15 2020
- Hayles NK (2017) *Unthought: the power of the cognitive nonconscious*. The University of Chicago Press, Chicago
- Held M (2006) Smart technologies and the end(s) of law: novel entanglements of law and technology. Edward Elgar, Cheltenham
- Held V (2006) *The ethics of care: personal, political, and global*. Oxford University Press
- Hines A (2018) Magnet implants? Welcome to the world of medical punk. *The New York Times*. <https://www.nytimes.com/2018/05/12/us/grindfest-magnet-implants-biohacking.htm>. Accessed 10 Jan 2020
- House A (2014) The real cyborgs. *The Telegraph*. <http://s.telegraph.co.uk/graphics/projects/the-future-is-android/>. Accessed 10 Jan 202
- IEEE (2019) *The IEEE global initiative on ethics of autonomous and intelligent systems. Ethically aligned design: a vision for prioritizing human well-being with autonomous and intelligent systems*, 1st Edition. <https://standards.ieee.org/content/ieee-standards/en/industry-connections/ec/autonomous-systems.html>
- Jaspers K (1932) [1970] *Philosophy*, vol II. University of Chicago Press, Chicago
- Keshavarz M (2019) *The design politics of the passport: materiality, immobility, and dissent*. Bloomsbury
- Kosinski M, Wang Y (2018) Deep neural networks are more accurate than humans at detecting sexual orientation from facial images. *J Pers Soc Psychol* 114(2):246–257. <https://doi.org/10.1037/pspa0000098>
- Lagerkvist A (2017) *Existential media: toward a theorization of digital thrownness*. *New Media Soc* 19(1):96–110. <https://doi.org/10.1177/1461444816649921>
- Lagerkvist A (ed) (2019) *Digital existence: ontology, ethics and transcendence in digital culture*. Routledge, London. <https://doi.org/10.4324/9781315107479>
- Lagerkvist A (2020) Digital limit situations: anticipatory media beyond ‘the new AI era.’ *JDSR* 2(3):16–41. <https://doi.org/10.33621/jdsr.v2i3.55>
- Lagerkvist A (2022) *Existential media. A media theory of the limit situation*. Oxford University Press, New York
- Levinas E (1961 [1979]) *Totality and infinity. An essay on exteriority*. Springer Science & Business Media
- Lin J, Jongbin J, Sharad G, Skeem J (2020) The limits of human predictions of recidivism. *Sci Adv*. <https://doi.org/10.1126/sciadv.aaz0652>
- Lupton D (2016) *The quantified self*. Polity, Oxford
- Lupton, D (2017) *The quantified self*. Wiley, Hoboken
- Lury C, Day S (2019) Algorithmic personalization as a mode of individuation (2019). *Theory Cult Soc* 36(2):17–37. <https://doi.org/10.1177/026327641881888>
- MacKenzie C, Stoljar N (eds) (2000) *Relational autonomy: feminist perspectives on autonomy, agency, and the social self*. Oxford University Press, New York
- Magnet S (2011) *When biometrics fail: gender, race, and the technology of identity*. Duke University Press, Durham
- Merleau-Ponty M (2014) *Phenomenology of perception*. Routledge, Oxon
- Noble S (2018) *Algorithms of oppression: how search engines reinforce racism*. NYU Press, New York
- Noddings N (1984) *Caring: a relational approach to ethics and moral education*. University of California Press, London
- Norlock K (2019) *Feminist ethics*. In: Zalta EN (ed) *The Stanford encyclopedia of philosophy* (Summer 2019 Edition). <https://plato.stanford.edu/archives/sum2019/entries/feminism-ethics/>
- O’Neil C (2016) *Weapons of math destruction: how big data increases inequality and threatens democracy*. Crown, New York
- Peters JD (2015) *The marvelous clouds: toward a philosophy of elemental media*. University of Chicago Press, Chicago
- Pfeifer M (2021) *Intelligent Borders? Securitized Smartphones in the European Border Regime*. *Culture Mach* vol. 20. <https://culturemachine.net/vol-20-machine-intelligences/intelligent-borders-securitizing-smartphones-in-the-european-border-regime-michelle-pfeifer/>
- Puig de la Bellacasa M (2017) *Matters of care: Speculative ethics in more than human worlds*. University of Minnesota Press, Minneapolis
- Ruddick S (1989) *Maternal thinking: toward a politics of peace*. Beacon Press, Boston
- Thacker, E (2004) *Biomedica*. University of Minnesota Press, Minneapolis
- Tronto JC (1993) *Moral boundaries: a political argument for an ethic of care*. Routledge, New York
- U.S. Department of Homeland Security (2016) ICE investigative case management DHS/ICE/PIA-045. <https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-icm-june2016.pdf>. Accessed 15 Mar 2020
- Vallor S (2016) *Technology and the virtues: a philosophical guide to a future worth wanting*. Oxford University Press, New York
- Verbeek PP (2011) *Moralizing technology: understanding and designing the morality of things*. The University of Chicago Press, Chicago
- World Economic Forum (2020) *A framework for responsible limits on facial recognition*. http://www3.weforum.org/docs/WEF_Framework_for_action_Facial_recognition_2020.pdf. Accessed 1 Feb 2020
- Zuboff S (2019) *The age of surveillance capitalism: the fight for a human future at the new frontier of power*. Profile Books, London
- Zweig K (2022) *An Algorithm has no sense of tact* (MIT Press, 2022): Ein Algorithmus hat kein Taktgefühl: Wo künstliche Intelligenz sich irrt, warum uns das betrifft und was wir dagegen tun können. [An Algorithm has no sense of tact: where AI makes mistakes, why that affects us, and what we can do about it]. Heyne Verlag, München 2019
- Zylinska J (2014) *Minimal ethics for the Anthropocene*. Open Humanities Press, London

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.