Special Issue

Decolonizing Privacy Studies

Television & New Media
1–13

DOI: 10.1177/1527476418806092
journals.sagepub.com/home/tvn
SAGE

Payal Arora[1]

Abstract

This paper calls for an epistemic disobedience in privacy studies by decolonizing the approach to privacy. As technology companies expand their reach worldwide, the notion of privacy continues to be viewed through an ethnocentric lens. It disproportionately draws from empirical evidence on Western-based, white, and middle-class demographics. We need to break away from the market-driven neoliberal ideology and the Development paradigm long dictating media studies if we are to foster more inclusive privacy policies. This paper offers a set of propositions to de-naturalize and estrange data from demographic generalizations and cultural assumptions, namely, (1) predicting privacy harms through the history of social practice, (2) recalibrating the core-periphery as evolving and moving targets, and (3) de-exoticizing "natives" by situating privacy in ludic digital cultures. In essence, decolonizing privacy studies is as much an act of reimagining people and place as it is of dismantling essentialisms that are regurgitated through scholarship.

Keywords

decolonial, privacy studies, surveillance, datafication, digital culture, big data, global South

Introduction

Privacy studies is in its heyday. What was once on the fringes of multiple disciplines is now centerfold and for good reason. Innovations such as social media, ubiquitous computing, mobile platforms, and smart technologies are increasingly datafying our lives. Big data analytics capitalizes on these massive datasets to address previously intractable problems across wide-ranging fields including health care, education,

[1]Erasmus University Rotterdam, The Netherlands

Corresponding Author:
Payal Arora, Associate Professor and Founder and Executive Director of Catalyst Lab, Erasmus School of History, Culture and Communication, Erasmus University Rotterdam, Room M8-10, Burgemeester Oudlaan 50, 3062 PA Rotterdam, The Netherlands
Email: arora@eshcc.eur.nl

retail, and banking. While this has yielded enormous benefits for the state and the market, it has alarmingly come at the cost of privacy (Cohen 2012).

This has led to the burgeoning of studies from diverse disciplines in the last decade to gauge what privacy is "worth" to individuals (Acquisti et al. 2013; Heikkilä 2018; Kokolakis 2017). Implicit in this body of research is the notion of privacy as a currency, as a rational trade-off, and as an exchange value to enable policy makers, legal scholars, and businesses to estimate how much customers care about the protection of their personal data. Privacy studies has come to be dominated by this capitalistic worldview. Privacy as a value is subsumed by market logic. This is embedded in the prevailing "dataism" ideology of objectivity arising from the quantification of our social behavior, revealing insights into our personal lives (van Dijck 2014).

In recent years, a number of scholars have sounded the alarm on the mythologies perpetuated by big data claims, and the normalizing of the "privacy rich" and "privacy poor" divides in access, management, ethics, representation, and interpretation (Arora 2016; Boyd and Crawford 2012; Couldry and Powell 2014; Milan and Trere 2017a; Pasquale 2015). There is a demand to estrange data from demographic generalizations and question underlying cultural assumptions, providing privacy its "contextual integrity" (Nissenbaum 2009). Of particular concern are the new forms of discrimination emerging through predictive data analytics, marginalizing the already vulnerable subjects of society (Leurs and Shepherd 2017). Studies on privacy harms through datafication such as racial profiling and policing (Noble 2018), biometric surveillance in the postcolonial context (Arora 2016), and state automation of welfare systems (Eubanks 2018), have pushed this agenda further.

At the heart of this momentum is a call to recognize the deeply structured, essentializing and historically reproduced power asymmetries within social and technical norms, knowledge, values, and infrastructures and counter this by pushing forward the notion of the "South" as "resistance, subversion and creativity as responses to situations of marginalization of various kinds" (Milan and Trere 2017b). This essay responds to this call, particularly on the sidelining of the Global South as it pertains to privacy studies.

The Need for an Epistemic Disobedience in Privacy Studies

Fuchs argues that we need to counter the colonization of the social media terrain to strive for a "commons-based media" (Fuchs 2015, xii). Colonization here is defined more broadly, where the "imperatives of autonomous subsystems make their way into the lifeworld from the outside—like colonial masters coming into a tribal society—and force a process of assimilation upon it" (Habermas 1984, 355). While this is surely a critique against the existing capitalist order, it also implies the possibility of a reversal through the process of *decolonization* using communicative action, that which "substitutes the systemic logic of money and power" with spaces of critical cooperation (Fuchs 2015, 64).

The evocation of colonialism is not a coincidence as we witness the rise of the next billion users outside the West, where more than 85 percent of the world's youth reside (Arora, forthcoming). Cheap mobile phones and diverse data plans have enabled the eager and curious young people in these nations to connect, socialize, and disclose much of their personal lives online. The techno-oligarchs such as Facebook, Twitter, Amazon, and Google are computing data of much of this region given the weak or nonexistent privacy and data protection laws. This expansionist outreach of pervasive datafication of the "peripheries" by the "core" can be viewed as a "colonial impulse" (Dourish and Mainwaring 2012, 135).

In spite of this global momentum of techno-empire building, privacy studies continues to be ethnocentric for the most part. It disproportionately draws from empirical evidence on privacy attitudes and behaviors of Western-based, white, and middle-class demographics to theorize privacy in this digitally mediated world (Chakravartty et al. 2018; Taylor 2017). Partly, this is a *disciplinary fracture*. Media studies, like its parent disciplines of sociology and political science, continues to focus on the north and leaves southern dynamics to be framed in terms of development.

This is problematic given that the field of development studies sprung from the "Development project," the institutionalization of a hegemonic template on "progress" for developing countries by Western and elite transnational organizations (McMichael 2011). It arguably extended colonialism through economic nationalism and neoliberal marketization, entrenching the status quo of the unequal world order (Duffield and Hewitt 2013). More than any other humanities and social sciences field, this discipline partners with the governments, technology companies, and elite multilateral organizations, and often uses the Global South public in "low-rights environments" as testbeds for innovations in technological surveillance (Eubanks 2014, 3). Privacy concerns thereby would be marginal to this agenda.

Partly, this is due to the perpetuation of the *exotification of subjects* outside the West. The lived lives of Global South communities, be it their privacy perceptions, harms, values, and norms, are seen as too distant to be relevant to those pursuing reforms in the design of socio-technical systems within the Global North (Mano and Willems 2017). This exceptionalism, the "us" versus "them" narrative, and the essentializing of entire groups and peoples as distinct and "othered" have long served the knowledge-making of the West (Said 1979).

This can lead to knee-jerk reductionisms of the motivations and consequences of privacy practice outside the West. For instance, the Meeker report on Internet trends found that different cultures demonstrate remarkably different levels of public sharing (Arora, forthcoming). Sixty percent of Saudis reported that they shared "everything" or "most things" online, compared with 15 percent in the United States and 10 percent in France, leading to the popular framing that these cultures do not care about their privacy as much as those in the West.

Most common, however, is defaulting to universalisms as part of the *inclusive capitalism and globalization approach to privacy* (Borko 2016). For example, the European Union's General Data Protection Regulation (GDPR) intends to spread their "golden standard" on privacy rules worldwide by applying these data regulations across

borders (Albrecht 2016). While well intended, it fails to acknowledge the fact that the term privacy has no direct translation in most of the world's languages and that there are few studies on what this means to the world's global public as they come online, share passwords, become visible, and at times stay anonymous (Miller et al. 2016).

This puts nations in the Global South at a disadvantage as it leaves little scope to institute indigenous privacy norms into their sociotechnical systems. Their fledgling technology industry has to deal with the emergence of national privacy and data protection laws. These states have few enforcement mechanisms, and the GDPR emphasis on individual choice assumes a high digital literacy among citizens and organizations. Thereby, GDPR, in spite of the good intent, could inadvertently hinder the Global South's digital participation and become a neocolonial entity instead.

Hence, it is important to adopt a decolonial approach to privacy by unpacking the ideological apparatuses in place and paying heed to the emerging forms of resistances. This essay goes against a privacy fundamentalism as it asks questions such as for whom is privacy a coherent concept? Whose privacy is negotiated and why? Whose privacy experience is stable and coherent? Given the dearth of privacy research in the context of the Global South, it makes the special case to embark on thoughtful analysis beyond the Development paradigm. While the Global South is diverse, vast, and "everywhere," it is also "always somewhere, and that somewhere, located at the intersection of entangled political geographies of dispossession and repossession, has to be mapped with persistent geographical responsibility" (Sparke 2007, 117).

This paper proposes the dismantling of key essentialisms embedded in privacy studies and affirms a "concrete universal into which all particulars are deposited" (Grosfoguel 2017, 96). At the center of this process is the questioning of the normative understandings of selfhood, community, and nation, juxtaposed against the territorial, ownership and propertied notions that pervade privacy discourse.

Mapping the Privacy Terrain

Depending on the field, specific notions of privacy are emphasized. For example, computer scientists focus on data security (Gürses and del Alamo 2016), while legal practitioners focus on civil liberties and the right to self-determination (Cohen 2012). The challenge here is to debunk the common argument that privacy is anti-innovative and static in this information age. Cohen offers a vibrant definition of privacy, in sync with the decolonial approach, namely, that which shelters a "dynamic, emergent subjectivity from the efforts of commercial and government actors to render individuals and communities fixed, transparent, and predictable" and protects "the situated practices of boundary management through which the capacity for self-determination develops" (p. 1905).

Some scholars frame privacy as a *choice* rooted in particular contexts (Nissenbaum 2009), while others characterize it as an *instrument* to free oneself from certain kinds of intrusions (Rachels 2017). Privacy can evoke a negative connotation of *concealment*, eliciting the popular defense on having "nothing to hide" when sharing data (Acquisti et al. 2016). It can just as well be the opposite, as a form of activism and

protest against the digital surveillance system through *obfuscation*—evasion, noncompliance, refusal, and even sabotage by average users to re-exert control over data about ourselves (Brunton and Nissenbaum 2015).

Many scholars treat privacy as relational in a sociological sense, where privacy is enacted in relation to other individuals and institutions—for example, unpacking the private against the digital public sphere (Quinn and Papacharissi 2017), the intimate against the demand to build social capital online (Balleys and Coll 2017), privacy concerns contradicting privacy behavior dubbed the "privacy paradox" (Marwick and Hargittai 2018), and the personal against the political as dissent becomes blurred with the mundane on social media (Yang and Jiang 2015).

Another classic tension lies between anonymity and transparency. Nissenbaum (1999, 27) defends the value of anonymity and reminds us that its value lies, "not in the capacity to be unnamed but in the possibility of action or participation while remaining out of reach or remaining unreachable." However, other scholars retort that by itself, anonymity is not virtuous nor is it an argument against transparency, and should not be overvalued at the expense of seeing the benefits of limited privacy (Coleman 2014).

There are, however, multiple privacy faultlines. Feminist studies have long resisted the notion of privacy as choice given the historical relegation of women into the domestic sphere (Gavison 1992). Privacy within this context can be a mode of oppression by patriarchal systems, and not subject to personal choice. Furthermore, the relation between privacy and morality is dominantly gendered, where social norms often overtake consent. This is captured by a growing body of literature on women viewed as property and tied to family and social honor, adding a layered vigilance on their digital behavior and reputation (Arora and Scheiber 2017). A woman can lose her right to privacy if perceived to have broken social conventions by traditional gate-keepers of social morality, such as religious institutions. Hence, decolonizing requires us to purge dichotomous thinking and view, instead, each entity within its own sociocultural and historical ecology, or baggage if you may.

Another dominant divide is between the individual and the institutional (Westin 2003). For example, an authoritarian society would take on a more paternalistic role in the individual's privacy, viewing their privacy as antithetical to social harmony. On the other hand, a capitalist system while favoring individual freedom and expression, would view privacy as a barrier to innovation. Although clearly distinct systems, they both disregard individual privacy within their own logic. The decolonizing of these constructs entails a centering of agency in their political systems. An emerging body of digital activism work affirms how acting within the digital realm intersects with lived experiences, fostering new collective identities that contest conventional, communal, and autonomous selves (Dencik et al. 2016; Yang and Jiang 2015). The decolonial approach resists framing of collectively held privacy values, focusing instead on people's capability and their freedoms to achieve (Sen 2000) and their capacity to aspire (Appadurai 2004) privacy in spite of constrained conditions.

It appears, therefore, that there is no overarching conception of privacy, as "it must be mapped like terrain, by painstakingly studying the landscape" (Solove 2008, x). It

is envisioned as less of a set of shared values and more as diverse values, which demand not assimilation but pluralism. Furthermore, it is tempting to dismiss the question of whether global privacy cultures pervade our contemporary lives. That would be a mistake. As we map privacy terrain, we should incorporate the ongoing global politics of territorial possession and empire building. While, indeed, we need to dismiss the universal "grammars" (Mbembé 2001, 41:9) of privacy, we need "provocative generalizabilities" (Fine 2012, 420) to move privacy studies forward. We need to escape the dilemma between isolated provincial particularisms and abstract universalisms on privacy by deepening reflexivity and our political imagination of locations, articulations, and movements at the margins.

Hence, below are specific propositions to decolonize privacy practice to strive for provocative generalizability, namely, (1) predicting privacy harms through the history of social practice, (2) recalibrating the core-periphery as evolving and moving targets, and (3) de-exoticizing "natives" by situating privacy in ludic digital cultures.

Predicting Privacy Harms through the History of Social Practice

Samira in a Gujarat slum hesitates to declare that she is Muslim for the Indian government's new biometric identity scheme that matches social benefits with digital identities. Given the contentious Hindu-Muslim history and past targeted Muslim persecutions by Hindu extremists using state databases, this trepidation seems understandable. Johan from a township in Cape Town is nervous about the launch of South Africa's Smart ID as it evokes past identification systems such as the Population Registration Act by the apartheid government used to racially segregate citizens. These are examples of rising privacy concerns of possible harms resulting from new state-driven datafication governance systems of their citizen identities (Arora 2016).

These apparatuses of so called efficiency and empowerment are built on information infrastructures with a colonial lineage. Information and control have a long-standing relationship. During the mid-nineteenth century, to police colonies, the British pioneered biometric surveillance through fingerprinting (Arora, forthcoming). The fear of an uprising was a constant motivator to identify and track their "unruly" subjects. In the case of India, the British matched privileges with caste, and inscribed this within the databased structure to be accessed through fingerprints. This perpetuated and deepened caste divisions.

Today, data on land records in India capture information not only about tenancy and the type of land titles but also about the age, caste, political registration, and religion of owners and tenants. The recording and sorting of the self may not per se lead to an invasion of privacy. However, the intersectionality of caste and land can be a privacy violation when a government official chooses to deny services to a citizen based on their caste.

At this juncture, it is worth taking pause on how to decolonize this analysis. While there is much emphasis on the unknown consequences from "predictive privacy harms" (Crawford and Schultz 2014), the decolonial approach would emphasize the "known" through the historicity of caste politics, for instance. We do not need novel

evidence that is databased to predict exploitation and the reifying of certain groups if we do the job of paying heed to the legacies of exclusion. Caste is an unredeemable social hierarchy that has no place in the modern world, regardless of the nature of the information, datafied or not.

Datafication is not an experiment but part of a long historical trajectory of institutionalizing the disciplining of subjects through technocratic means. We need to balance the fear of the unknown with the historical scrutiny of that which is tried and tested in sustaining privacy violations. We need to look at the colonial project, a geopolitical "success" in the reordering and sustaining of power relations, as a metaphor as well as an infrastructure for contemporary techno-empire making that pervades today.

For instance, we have much to learn from the centuries of "divide and rule" of social sorting and the rhetorical invention of the "barbaric natives" in need of civilizing to justify control (Arora, forthcoming). By framing the colonized as more primal in their needs, wants, and desires, the exotification served to normalize these group relations and universalize western values. The rationale of care, "the white man's burden" and not profit provided a paternalistic sheen and diverted attention from the market-driven mechanisms at play. Imperialism appeared as an obligation to humanity and that of a higher calling. The infantilizing of these subjects allowed the colonizers to exclude the natives from rights deserving of an individual. Those who challenged these universalisms became pathological subjects that needed further disciplining.

By this historical vignette, we can predict how the alliances of a select number of technology companies in complicity with the state can exercise their ideology and surveillance on entire publics. Privacy studies would benefit from channeling their energies not just on futuristic predictions but on past realizations that have benefited from the manufacturing of social divides.

Recalibrating the Core-Periphery as Evolving and Moving Targets

Unlike the West where the welfare recipients are in the minority, postcolonial nations are inherently development states with a significant poverty base. They claim to build their datafied identity systems to service the poor and the disenfranchised (Sarkar 2014). There is a case to be made as many of these nations struggle to serve their vast underprivileged citizens who are for the most part undocumented. There have been major achievements of inclusivity in the banking, education, and social benefit system, albeit at the price of privacy. Maslow's pyramid of needs re-imagines itself through the prioritization of digital identification and participation over privacy. We witness this again with Facebook's spread of Free Basics, an initiative offering free access to limited sites to the world's poor, while breaking net neutrality laws (Mano and Willems 2017).

However, this linear narrative of the North core subjugating the South periphery gets disrupted with the rise of the BRICS nations (Brazil, Russia, India, China, South Africa). This phenomena has produced new modes of intra-imperial competition, with China and its own techno-oligarchs such as Baidu, Alibaba, and Tencent leading the

way in building "infrastructures of empire" (Aouragh and Chakravartty 2016). Today, Chinese Internet firms are competing against old colonial powers, viewing Africa, for instance, as China's second continent (Jiang and Esarey 2018).

The emergence of the BRICS coalition and, at times, their imperial complicity pushes us to complicate Eurocentric narratives of empire building, and cautions us to not essentialize the West. Privacy violations can just as well come from within the traditional periphery. For example, the African postcolonial experiments in the 1950s to "Africanize" their nations resulted in politicizing identity over citizen well-being, performing more ideological than structurally transformative work (Fanon 2007). This entailed the re-application of logics of racial hierarchy and exclusion within African/postcolonial societies, led by power-hungry elites. Instead of this kind of inverted racism, we need to repossess one's humanity and dignity regardless of one's national or group affiliation, in this case, through the exercise of the right to privacy.

This does not negate the fact that Western technology companies have long benefited from their colonial relations and institutions and have proliferated their knowledge as the norm. While power asymmetries exist and are often relatively stable and reproductive, the core and the periphery can be moving targets that evolve alongside shifts in geopolitics. It thereby helps to pay more attention to similarity over difference between imperialist entities, whether they are home-grown or elsewhere. By embedding a plasticity in privacy conceptions, it allows us to move with the evidence and de-thaw frozen identities as we critique the datafication of citizens at the margins.

De-exoticizing Natives by Embedding Privacy in Ludic Digital Cultures

In 2013, Eric Zimmerman, a game designer, provoked the media through the launch of the "Manifesto for a Ludic Century" (Zimmerman 2015). He declared that play defines the twenty-first-century culture. The individual is a constant player, and life is his or her constant game. He attributes this to the new technologies that have risen around us, embedding us in a deluge of information. Given its infinite form, we are compelled to make our way through it for socializing, schooling, romancing, banking, and other mundane activities. Play is the figuring out of the rules of the game. New technologies constantly redefine the game, keeping play in a constant state of flux. Life is gamified. By thinking of life as play, privacy decision-making is viewed as mediated by the uncertainties structured in.

Ludification of our techno-induced culture is seen as accelerating, accentuating, and inscribing the compulsive need for play in our daily social interactions (Sicart 2014). Digital play is seen as our second nature today. However, inherent to this worldview is an idealistic and universalistic notion of play. This romanticism draws its inspiration from Huizinga's proposition of the "Homo Luden" where he espoused how play, in its purest form, has no practical utility and is the essence of a higher order civility (Huizinga 2014).

There is, however, an assumption of free will that dictates this manifesto. The fact is that the world's majority are often compelled to follow the rules of the game created by those in power. Laws and regulations are often aligned with the sustaining of social

inequality. Thereby, privacy, in such a context, is not necessarily voluntary nor self-gratifying. The fetishization of choice in play evades the expansive interpretations of privacy as a struggle, an exploitation and a means of survival. While this manifesto emphasizes abundance through new technology, playful privacy may be more as a response to scarcity. When the marginalized pioneer new ways of obfuscation, it is often viewed more as a deviant act than that of playfulness.

Situating privacy within ludic digital cultures can reveal needs and wants that are prosaic, unremarkable, and commonplace, such as seeking for friends and romance. This kind of digital play is especially useful to re-humanize those at the margins. It is what makes us all human. Play stimulates empathy for those at the margins as we learn how their desires, aspirations, and purposelessness to be public or private manifest, in spite of their constrained environments, and enable them forward. Decolonizing privacy studies is as much an act of reimagining people and place as it is of dismantling essentialisms that are regurgitated through scholarship. Users in the Global South continue to be fictionalized in their privacy behaviors and attitudes due to limited empirical evidence.

As mentioned earlier, studies on social media and Internet usage in these regions have been driven by development agendas with a strong historical bias toward socioeconomic ends. Particularly, low-income people in the Global South have been looked upon as primarily rational beings, driven by utilitarian outcomes. It is assumed that farmers adopt mobile Internet technologies to check crop prices and women primarily check health and education information on the Internet for their children. However, in recent years, scholarship has emerged that contests these constructs as they reveal that these users, in spite of their significant socioeconomic and cultural constraints, are motivated dominantly by leisure to adopt and sustain new digital practice, much like the everyday Western user (Gajjala and Tetteh 2014; Ganesh 2010; Tully and Ekdale 2014). Their online datafied behaviors are steeped in romance, sociality, entertainment, gaming, and pornography. By focusing on their everyday practice, it

> . . . will help us focus on the heterogeneous and life-enhancing aspects of technological use encompassing both experiential and purposive elements of ICT adoption. Leisure is a critical area of technology infusion that leads to discovery and magnification of digital literacies. Moreover, leisure offers an experimental space to informally diffuse learnings and impart social impacts that bind people and technologies. (Arora and Rangaswamy 2013, 899)

Hence, by repositioning privacy within the everyday and contemporary practices of media consumption driven by play, pleasure, and entertainment, we can gain insight into the privacy aspirations, tactics, and literacies of these long fictionalized users.

Concluding Thoughts

The growth of data analytics has induced the growth of data metrics. Meaning-making seems to emerge from the computing of digital presentation and behavior to best gauge

the data's influence and impact on the self and society. The monetization of engagement involves the commodification of privacy, as users are pushed to optimize their selves and their networks to serve the neoliberal ethic of productivity. The prevalent "vanity metrics" of valorising visibility, sharing, and publicness to garner higher social status (Rogers 2018) does not privilege privacy within its rubric.

This paper challenges the hegemony of metrics in privacy studies with a more expansive, interdisciplinary and inclusive approach, much in alignment with this special issue call to adopt a "Southern" perspective. This essay offers key propositions to chart our way forward to dignify those at the margins, by giving their privacy its contextual integrity. While the focus has been on the marginalization of the Global South in these efforts, this proposition is transferrable to any other marginal entity as they all encompass their narratives of creative insurgencies.

We need to recognize that while we embark on this approach, we may encounter the tension between individual and group privacy that emerges from datafication. Instead of discounting one against the other, we should sensitize ourselves to the different disciplinary biases when approaching privacy. For instance, marketing, business, and innovation research would benefit from the reminder of the negative discrimination of a certain kind of group profiling, especially as they deal with data aggregates. On the other hand, critical data studies should recognize that in their social justice advocacy for positive discrimination, this may inadvertently freeze individual and group identities.

In pushing for a provocative generalizability, this paper makes the case that decolonial scholars should not shy away from the particularities of globalization of privacy values, norms, and practices while dismantling pervasive universalisms in the process. By shifting our attention to digital ludic cultures and playfulness, we can better understand the interweaving of the need to be seen with the need to be hidden, without resorting to a binary approach or paradoxical framing. While this essay makes the case to reconfigure normative understandings on privacy by looking across borders, the Global South is no monolithic entity. For example, it is not unified on matters of sexuality, moral codes of conduct, policing, and gender rights.

Privacy as a value should not be predetermined. We need to open our purview to alternative meanings including paying heed to the desire for selective visibility, how privacy is often not a choice, and how the cost of privacy is deeply subjective and seemingly irrational as desire and aspiration overtakes pragmatism. Subjects need to go beyond the parameters of the researcher's interests to become de-subjectified, or better yet, de-exoticized.

Declaration of Conflicting Interests

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

Funding

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

References

Acquisti, Alessandro, Leslie K. John, and George Loewenstein. 2013. "What Is Privacy Worth?" *The Journal of Legal Studies* 42 (2): 249–74. doi:10.1086/671754

Acquisti, Alessandro, Curtis Taylor, and Liad Wagman. 2016. "The Economics of Privacy." *Journal of Economic Literature* 54 (2): 442–92.

Albrecht, Jan Philipp. 2016. "How the GDPR Will Change the World." *European Data Protection Law Review* 2: 287–89.

Aouragh, Miriyam, and Paula Chakravartty. 2016. "Infrastructures of Empire: Towards a Critical Geopolitics of Media and Information Studies." *Media, Culture & Society* 38 (4): 559–75.

Appadurai, Arjun. 2004. "The Capacity to Aspire: Culture and the Terms of Recognition." In *Culture and Public Action*, edited by Vijayendra Rao and Michael Walton, 59–84. Palo Alto: Stanford University Press.

Arora, Payal. 2016. "The Bottom of the Data Pyramid: Big Data and the Global South." *International Journal of Communication* 10 (January): 1681–99. doi:1932–8036/20160005

Arora, Payal. Forthcoming. *The Next Billion Users: Digital Life beyond the West*. Cambridge: Harvard University Press.

Arora, Payal, and Nimmi Rangaswamy. 2013. "Digital Leisure for Development: Reframing New Media Practice in the Global South." *Media, Culture & Society* 35 (7): 898–905.

Arora, Payal, and Laura Scheiber. 2017. "Slumdog Romance: Facebook Love and Digital Privacy at the Margins." *Media, Culture & Society* 39 (3): 408–22.

Balleys, Claire, and Sami Coll. 2017. "Being Publicly Intimate: Teenagers Managing Online Privacy." *Media, Culture & Society* 39 (6): 885–901.

Borko, Henryk. 2016. "Inclusive Capitalism: Economic Development or Stagnation? A Regional Perspective." *Tiltai* 74 (2): 33–52. doi:10.15181/tbb.v74i2.1365

Boyd, Danah, and Kate Crawford. 2012. "Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon." *Information, Communication & Society* 15 (5): 662–79.

Brunton, Finn, and Helen Nissenbaum. 2015. *Obfuscation: A User's Guide for Privacy and Protest*. Cambridge: MIT Press.

Chakravartty, Paula, Rachel Kuo, Victoria Grubbs, and Charlton McIlwain. 2018. "# CommunicationSoWhite." *Journal of Communication* 68 (2): 254–66.

Cohen, Julie E.. 2012. "What Privacy Is for." *Harvard Law Review* 126:1904.

Coleman, Gabriella. 2014. *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*. Brooklyn: Verso Books.

Couldry, Nick, and Alison Powell. 2014. "Big Data from the Bottom Up." *Big Data & Society* 1 (2): 1–5. doi:10.1177/2053951714539277

Crawford, Kate, and Jason Schultz. 2014. "Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms." *Boston College Law Review* 55:93–128.

Dencik, Lina, Arne Hintz, and Jonathan Cable. 2016. "Towards Data Justice? The Ambiguity of Anti-Surveillance Resistance in Political Activism." *Big Data & Society* 3 (2): 1–12. doi:10.1177/2053951716679678

Dourish, Paul, and Scott D. Mainwaring. 2012. "Ubicomp's Colonial Impulse." In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*, 133–142. Pittsburgh, USA: Association for Computing Machinery.

Duffield, Mark, and Vernon Hewitt. 2013. *Empire, Development & Colonialism: The past in the Present*. Woodbridge: Boydell & Brewer.

Eubanks, Virginia. 2014. "Want to Predict the Future of Surveillance? Ask Poor Communities." *The American Prospect*, January 15. http://prospect.org/article/want-predict-future-surveillance-ask-poor-communities.

Eubanks, Virginia. 2018. *Automating Inequality: How High-tech Tools Profile, Police and Punish the Poor*. New York: St. Martin's Press.

Fanon, Frantz. 2007. *The Wretched of the Earth*. New York: Grove/Atlantic.

Fine, Michelle. 2012. "Resuscitating Critical Psychology for 'Revolting' Times." *Journal of Social Issues* 68 (2): 416–38.

Fuchs, Christian. 2015. "Social Media and the Public Sphere." *tripleC: Open Access Journal for a Global Sustainable Information Society* 12 (1): 57–101.

Gajjala, Radhika, and Dinah Tetteh. 2014. "Relax, You've Got M-PESA: Leisure as Empowerment." *Information Technologies & International Development* 10 (3): 31–46.

Ganesh, Indira Maya.2010. "'Mobile Love Videos Make Me Feel Healthy': Rethinking ICTs for Development." *IDS Working Papers* 2010 (352): 1–43. doi:10.1111/j.2040-0209.2010.00352_2.x

Gavison, Ruth. 1992. "Feminism and the Public/Private Distinction." *Stanford Law Review* 45:1–45.

Grosfoguel, Ramón. 2017. "Decolonizing Western Universalisms: Decolonial Pluri-Versalism from Aimé Césaire to the Zapatistas." In *Towards a Just Curriculum Theory*, edited by João M Paraskeva, 159-76. London: Routledge.

Gürses, Seda, and Jose M. del Alamo. 2016. "Privacy Engineering: Shaping an Emerging Field of Research and Practice." *IEEE Security & Privacy* 14 (2): 40–6.

Habermas, Jürgen. 1984. *The Theory of Communicative Action*. Vol. 1. Boston: Beacon Press.

Heikkilä, Heikki. 2018. "Privacy under Surveillance: Towards a Conceptual Analysis of the Price of Connection." *Northern Lights: Film & Media Studies Yearbook* 16 (1): 59–74.

Huizinga, Johan. 2014. *Homo Ludens Ils 86*. London: Routledge.

Jiang, Min, and Ashley Esarey. 2018. "(Un) Civil Society in Digital China| Uncivil Society in Digital China: Incivility, Fragmentation, and Political Stability—Introduction." *International Journal of Communication* 12:1928–44.

Kokolakis, Spyros. 2017. "Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon." *Computers & Security* 64:122–34.

Leurs, Koen, and Tamara Shepherd. 2017. "15. Datafication & Discrimination." In *The Datafied Society: Studying Culture through Data*, edited by Mirko Tobias Schäfer and Karin van Es, 211–32. Amsterdam, The Netherlands.

Mano, Winston, and Wendy Willems. 2017. "Decolonizing and Provincializing Audience and Internet Studies: Contextual Approaches from African Vantage Points." In *Everyday Media Culture in Africa: Audiences and Users*, edited by Wendy Willems and Winston Mano, 15–40. London: Routledge.

Marwick, Alice, and Eszter Hargittai. 2018. "Nothing to Hide, Nothing to Lose? Incentives and Disincentives to Sharing Information with Institutions Online." *Information, Communication & Society*. Published electronically March 29. doi:10.1080/1369118X.2018.1450432

Mbembé, J.-A. 2001. *On the Postcolony*. Vol. 41. Berkeley: University of California Press.

McMichael, Philip. 2011. *Development and Social Change: A Global Perspective*. Newbury Park, CA: Sage.

Milan, Stefania, and Emiliano Trere. 2017. "Dataactive:The Politics of Data According to Civil Society." *Big Data from the South: The Beginning of a Conversation We Must Have*, October 16. https://data-activism.net/2017/10/bigdatasur/.

Miller, Daniel, Elisabetta Costa, Nell Haynes, Tom McDonald, Razvan Nicolescu, Jolynna Sinanan, Juliano Spyer, Shriram Venkatraman, and Xinyuan Wang. 2016. *How the World Changed Social Media*. London: UCL Press.

Nissenbaum, Helen. 1999. The meaning of anonymity in an information age. *The Information Society* 15 (2): 141–144.
Nissenbaum, Helen. 2009. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford: Stanford University Press.
Noble, Safiya Umoja. 2018. *Algorithms of Oppression: How Search Engines Reinforce Racism*. New York: New York University Press.
Pasquale, Frank. 2015. *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge: Harvard University Press.
Quinn, Kelly, and Zizi Papacharissi. 2017. "Our Networked Selves: Personal Connection and Relational Maintenance in Social Media Use." In *The SAGE Handbook of Social Media*, edited by Jean Burgess, Thomas Poell, and Alice Marwick, 353–71. New York: Sage.
Rachels, James. 2017. "Why Privacy Is Important." In *Privacy*, 11–21. Abingdon, OX: Routledge.
Rogers, Richard. 2018. Digital Traces in Context| Otherwise Engaged: Social Media from Vanity Metrics to Critical Analytics. *International Journal of Communication* 12: 23.
Said, Edward. 1979. *Orientalism*. New York: Vintage.
Sarkar, Swagato. 2014. "The Unique Identity (UID) Project, Biometrics and Re-Imagining Governance in India." *Oxford Development Studies* 44 (4): 516–33.
Sen, Amartya. 2000. "Development as Freedom." *Development in Practice, Oxford* 10 (2): 258–58.
Sicart, Miguel. 2014. *Play Matters*. Cambridge: MIT Press.
Solove, Daniel. 2008. *Understanding Privacy*. Cambridge: Harvard University Press.
Sparke, Matthew. 2007. "Everywhere but Always Somewhere: Critical Geographies of the Global South." *The Global South* 1 (1): 117–26.
Taylor, Linnet. 2017. "What Is Data Justice? The Case for Connecting Digital Rights and Freedoms Globally." *Big Data & Society* 4 (2): 1–14. doi:10.1177/2053951717736335
Tully, Melissa, and Brian Ekdale. 2014. "Sites of Playful Engagement: Twitter Hashtags as Spaces of Leisure and Development in Kenya." *Information Technologies & International Development* 10 (3): 67–82.
van Dijck, José. 2014. "Datafication, Dataism and Dataveillance: Big Data between Scientific Paradigm and Ideology." *Surveillance & Society* 12 (2): 197–208.
Westin, Alan F.. 2003. "Social and Political Dimensions of Privacy." *Journal of Social Issues* 59 (2): 431–53.
Yang, Guobin, and Min Jiang. 2015. "The Networked Practice of Online Political Satire in China: Between Ritual and Resistance." *International Communication Gazette* 77 (3): 215–31. doi:10.1177/1748048514568757
Zimmerman, Eric. 2015. "Manifesto for a Ludic Century." In *The Gameful World: Approaches, Issues, Applications*, edited by Steffen P. Walz and Sebastian Deterding, 19–22. Cambridge: MIT Press.

Author Biography

Payal Arora is the author of several books on the Internet and the Global South including "The Next Billion Users: Digital Life beyond the West" with Harvard University Press. She has published forty-five papers in her field and has given 125 presentations across seventy-three cities in thirty countries, including a TEDx talk on the future of the Internet. She is the founder of Catalyst Lab, a digital activism organization, and an associate professor at Erasmus University Rotterdam.