The Journal of Sociotechnical Critique

Volume 1
Issue 1 *Online First*

Article 1

May 2020

From protecting to performing privacy

Garfield Benjamin
Solent University, garfield.benjamin@solent.ac.uk

Recommended Citation

Benjamin, G. (2020). From protecting to performing privacy. *Journal of Sociotechnical Critique*, *1*(1), 1–30. Advance online publication. https://doi.org/10.25779/erx9-hf24

From protecting to performing privacy

Garfield Benjamin
Solent University

Privacy is increasingly important in an age of facial recognition technologies, mass data collection, and algorithmic decision-making. Yet it persists as a contested term, a behavioural paradox, and often fails users in practice. This article critiques current methods of thinking privacy in protectionist terms, building on Deleuze's conception of the society of control, through its problematic relation to freedom, property and power. Instead, a new mode of understanding privacy in terms of performativity is provided, drawing on Butler and Sedgwick as well as Cohen and Nissenbaum. This new form of privacy is based on identity, consent and collective action, a process to be performed individually and together to create new structures that instil respect at the heart of our sociotechnical systems.

Keywords: privacy, performativity, contextual integrity, data, identity, consent, power

The prevailing culture of privacy is centred on the assumption that it is something that needs to be protected. But this framing has mired privacy in fear and helplessness born of protectionist thinking. That is not to say that the affective impact of fear cannot be a force for radical change. Indeed, Sedgwick's (2003) performativity stems from affect, a collective process of feeling and learning, and thereby action. Critiquing protectionist privacy does not erase its importance, but acknowledges its basis as a call for change upon which performative conceptions can emerge as a constructive and collective contrast. But the privacy paradox shows that increased knowledge of threats does not inspire users to better protect themselves (Mamonov & Koufaris 2016; Black et al. 2018). Defensive perspectives tend towards a sense of inevitability, carried through cultural representations in film, literature, games and the press whereby privacy becomes a battle already lost to the all-powerful spectres of government, business or malicious hackers. And yet, privacy *is* worth protecting. Or, at least, it is worth ensuring users have control over access to their data and metadata if and when they want it. Privacy is a temporal and political issue, and the harms of new technologies are often distributed unequally and visible only in retrospect. How, then, can we support privacy without resorting to failed protectionism? There are a series of emerging debates and conceptions of privacy that are making progress towards this aim, which we here suggest can be best encapsulated as *performing privacy*.

Writing just before the recent swing back in favour of privacy—in the wake of mass surveillance revelations, social media data scandals and advances in facial recognition—Cohen found resistance to privacy (in

favour of the Silicon Valley rhetoric of innovation or post-9/11 government expansion of security powers) to be based on the problem that "legal scholarship has conceptualized privacy as a form of protection for the liberal self. So characterized, privacy is reactive and ultimately inessential" (Cohen, 2013, p. 1905). Cohen moves beyond the liberal self with a poststructuralist and social constructivist framework that emphasises the importance of performativity in the construction of the relational, multivalent, networked self of contemporary privacy (2012, p. 129). However, she refuses to endorse any particular theory (p. 147), and her use of performativity remains focused on the constructive process of identity formation and a deconstructive critique of sharing, rather than the constructive and reconstructive relational context in which privacy itself might be performed.

Cohen's position acts as a useful basis for positioning the subject(s) of privacy amidst the messiness, embeddedness and heterogeneity of culture (2012, p. 267). But performativity calls into question not only the liberal subject but also the emphasis on autonomy (see, for example, Butler & Athanasiou, 2013, p. 2) that underpins legal understandings of the subject. Examples such as regulating to enforce value-centred design —as the iterative construction of norms—therefore need pushing further into elaborating more explicitly performative enactments of privacy as a collective practice, moving beyond performative identity *and* privacy (Cohen, 2008, p. 187) towards a performative conception *of* privacy. In order to fully embrace a performative approach, and to collectively apply such an approach in practice, we must therefore move beyond asking what function privacy performs and instead ask how we can perform privacy together. That is the topic of this discussion.

The definition of privacy used in this article expands on Nissenbaum's concept of "contextual integrity" as appropriateness and flow (2004), later expanded to include contexts, norms, actors, attributes (types of information) and transmission principles (Nissenbaum, 2010, p. 129f), although to some extent these are all subsumed within both contexts and norms. Nissenbaum's framework offers a negotiation of the specificity and interrelatedness of different spheres or contexts and the new cultures that emerge therein (Nissenbaum, 2011, p. 38), it is both "heterogeneous and thickly integrated with social life" (p. 43). Integrated into all aspects of society, privacy cannot be compartmentalised (Nissenbaum, 2010, p. 128), for the flow of information is embedded in any human society through all levels of interaction. Contextual Integrity as a concept offers a relational and embedded definition of privacy which is usefully extended by thinking in terms of performativity, such as emphasising the temporal aspects of contexts as continued social engagement and (re)construction over time.

Building on gender theories of the performative and periperformative acts that constitute social structures (Butler, 1988, 2015; Sedgwick, 2003; Green, 2007) situates privacy simultaneously in the individual and at the root of broader systems of power. This article develops a performative understanding of privacy in order to move beyond the descriptive-normative divide, towards thinking privacy as an active process and thereby a more relevant framework for collective action. Skinner-Thompson (2017) explores performative privacy in a legal context, emphasising the act by individuals or groups of resisting surveillance in public as expressive acts: hoodies and physical masks, online identity masking tools, transgender rights, and head veils. An instructive development from this legal perspective is that "functional demands for privacy may also be viewed as legally-protected speech—as expressive" and also as political (p. 1726). This is a useful move towards sharing as a part of privacy, transcending the public-private divide, and establishing a regulatory basis for performing privacy as empowerment. The approach developed here pushes this argument further, beyond performing anti-surveillance, into a fuller contextual way of thinking that incorporates sharing and withholding, subject and audience, individual and collective, and interdisciplinarity. Performing privacy requires a simultaneous shift in all spheres: law, technology, ethics, politics, economics, and, perhaps most importantly, culture.

Protecting privacy

Protecting privacy is often described as a "losing battle" (Kerry, 2018), yet it persists as the focus of debates, particularly in technical and legal spheres. This is perhaps an artefact of those specific fields, the need for clearly definable terms and requirements for generalisable application and enforcement. But society is not uniform, there is no one-privacy-fits-all. By thinking solely in terms of technical and legal systems, we risk falling into a defensive, protectionist position that fails to empower individual agency by placing too much emphasis on broader structures. This escalation is where individual circumstances, particularly those of marginalised or underrepresented groups, get lost. It is therefore necessary to critique the relation of privacy to the existing (often exclusionary) frameworks of thought that are used to justify its problematic definition as something to be protected.

Freedom

The most obvious justification for protecting privacy is through its understanding in relation to freedom. In his highly influential text on privacy and freedom, Westin defines privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (2015 [1967], p.

7). This suggests a core understanding of privacy in terms of protecting freedom and the "right" to privacy, which is followed through in much legal scholarship that tends towards taxonomising these rights (Solove, 2005, 2008). Such taxonomisation is widespread, although not without limitations of contextual specificity and agent relativity (O'Callaghan, 2012, pp. 16-17). A necessary protection made all too clear in the aftermath of the Snowden revelations is from the state. This is of course an important endeavour, and one in which organisations like the Electronic Frontier Foundation, Privacy International, or Liberty Human Rights are essential. But beneath this very clear and very real need—particularly for groups historically persecuted by state apparatus (Browne, 2015) or to enable the ability of journalists and political activists to operate in oppressive states (Blum-Dumontet, 2019) - lies a problematic framework that places the individual always as victim, as subject to the state's grace.

Monitoring citizens has long been a function of the state, whether for taxation or control. Expecting privacy protections against the state will always be a qualified rather than absolute right, always easily traded for the interests of the state. This is further complicated by the blurred relations of access and privacy. For example, Rød and Weidmann show that "regimes aiming to prevent any independent public sphere are more likely to introduce the Internet" (2015, p. 338), while states with more democratic systems (such as the US or UK) have a tendency to escalate surveillance legislation disproportionate to their claims of promoting freedom. This suggests that enhanced internet freedom, for example, does not necessarily equate to enhanced privacy, building on the inherent tension between freedom of information and right to privacy that suggests a potential incompatibility with other freedoms.

If protecting privacy freedoms from governments is problematic, what of protection from platforms and corporate interests? Structurally, this is to some extent impossible. It is tech companies who collect, hold and process our information on a daily basis. It is tech companies who manage and control the infrastructure and platforms upon which digital society operates. If protection of privacy *from* governments cannot be relied upon, as we have seen, then it is also naive to expect protection of privacy *by* governments. Recent developments in the wake of the GDPR or the Facebook/Cambridge Analytica scandal have led to a push for regulation of big tech, but governments have been slow to act and have thus far shown little in the way of meaningfully challenging the dominance of major corporations. The underlying structure of freedom and rights in online reality is predicated on a fundamental power asymmetry between organisations (internet service providers, platforms, hardware manufacturers, but also governments) and individuals.

Another key area of freedom in which privacy protections must be understood is from other individuals and, taken together, society as a whole:

> Privacy provides the self shelter from the storm; it gives the nascent self the breathing space to develop, and the developed self a personal realm to exist as it is, free from the prying eyes and corrosive influence of society. (Hill, 2004, pp. 571-2)

At first glance, this situates privacy as a positive and empowering protection. But who decides which influences are deemed corrosive? This is particularly problematic when considering privacy from the family. Children's rights to privacy have recently been identified as an overlooked issue (Children's Commissioner for England, 2018), with parents and schools (those supposedly there to protect children) often forming part of the problem through sharing children's data on social media, normalising passive surveillance in education, or forcing engagement with privacy-invasive systems.

Privacy within and of the family unit is further problematised in relation to gender. Maintaining the privacy of the family home (dating back to Aristotle's public-private divide) has long been an act of concealing abuse, particularly of women. While bodily privacy is important for sexual rights and empowerment, it can also be used to protect systemic abusers, carried forward onto digital devices in the form of (legal) "stalkerware" or "spouseware" (Greenberg, 2019). Viewing privacy as protection—as freedom, and as the specific rights of a given legal framework—is a process of layering, prioritisation and discrimination. Whose freedom comes first? Sedgwick notes how performative frameworks and periperformative contexts (discussed below) can expose the risks of privacy in, for example, the violence of slavery within quasi-familial contexts (2003, p. 83). These issues of freedom are of course part of a long debate going far beyond privacy, but they call into question the justification of privacy as a protection. Thinking privacy in terms of protecting freedom will always be disproportionately ineffective for marginalised groups, amplifying existing inequalities in societies for which equal rights are a mythical ideal rather than an enforceable reality.

Privacy legislation is severely limited in practice. It relies on a patchwork of other rights and protections such as disability, genetic or other legislation (Horvitz & Mulligan, 2015), and remains "weak, incomplete, and fractured" (Bamberger & Mulligan, 2011, p. 249). Current regulation is merely an enforced minimum upon which individual organisations must build their own privacy framework (often finding legal loopholes, particularly for manipulating consent over time). Mulligan and Horvitz (2015) demonstrate how privacy can be used to help prevent discrimination by limiting access to information that could be used to discriminate (p. 253), but that the

same process can hinder the recognition of discriminatory classifications subsumed in other identifying pieces of information from which inferences generate discrimination (Dwork and Mulligan 2013, p. 37). An example of this is Facebook's differential advertising of real estate not explicitly grounded in race but still discriminatory by latching onto associated identifiers such as neighbourhood that racially stratify communities in practice.

Even the apparent protections of anti-discrimination discourse around bias in data and algorithms are often overly instrumental, based on "the liberal rubric of rights, opportunities, and material resources" (Hoffmann, 2019, p. 909) in which privacy is reduced to consumer rights rather than taking into account, for example, attacks on dignity. Hoffmann goes on to state that privacy is not a "panacea" (p. 910) for bias and data-based harms, but broadening the definition of privacy beyond a protectionist viewpoint could allow us to better embrace the embeddedness of different social and technological principles in how individuals are defined, operationalised, and (mis)treated with technology. Escaping the corporate definitions of privacy (and consent, discussed below) used for terms and conditions or PR stunts is an essential step. This would enable privacy to better support the project of addressing broader social inequalities and the pursuit of justice for marginalised groups.

But beyond these practical and systemic clashes within privacy, we can also ask whether privacy is even conceptually compatible with freedom. As Mokrosinska (2018) suggests, "privacy as control over access [...] is about normative control involving a moral claim on the part of the agents to limit the liberty of anyone else to search for information or to interfere with their decisions." In this understanding of access control—already narrowing its usefulness and undermined by, for example, the Right to Be Forgotten in which privacy comes into conflict with a host of other rights and public interests—privacy is in fact not a freedom but a limit on it. Privacy as normative control is an act of closing off, of separation. Thinking this way undermines the positive component of privacy and contextual integrity as also being concerned with sharing and the building of social connections.

Privacy may involve protection (of identity, of consent, of autonomy), but a protectionist rhetoric of privacy displaces these other concerns into a tradeable right that all too often loses out to grander concerns of the loci of power (whether in patriarchal family structures, corporate boards, or government agencies). But protecting privacy as a process of *individual* self-defense (Cohen, 2008, p. 201) also fails in the collective implications of information leakage or exploitation such as the similarities in genetic information of family members, the relational information of one's contacts or communication metadata, or the normalising effects of data *en masse*

as a tool for discrimination. Perhaps this is why privacy has been described as “the lost right” (Mills, 2008). Protecting privacy as a freedom fails at the limit of those protections, a brittle edge past which marginalised individuals and groups are easily abandoned.

Property

Personal data—and therefore the understanding of privacy—is increasingly defined as property. Igo highlights the 1960s as one of the “critical episodes” (2018b, p. 3) in which privacy came to be understood in terms of property (2018a), alongside the rise of the surveillance society (2015), forming a social shift that instigated new legal protections. While Igo’s broader history of privacy (2018b) remains US-centric and limited by the fallback to problematic legal discourses of autonomy and freedom, it is instructive on the two-sided anxieties of privacy. Igo importantly emphasises the sociocultural impact and breadth of the language of privacy debates, and its embeddedness within society (p. 6). Thinking about privacy as property is unhelpful not only when used by companies justifying access to data in return for access to services, but also in positive attempts to transfer ownership of data back to individuals, offering them the choice of whether, to whom and for how much to trade away their data. Fundamentally, this does nothing to question the economic power structures and access control. The “data is the new oil” rhetoric emphasises a transactional approach to privacy that, ultimately, only serves private (business) interests.

Zuckerberg’s declaration that “the future is private” (2019) therefore highlights an act of encryption-washing that protects privacy from government surveillance while making the future of data fully privat*ised* under corporate ownership. But data is not even treated as carefully or regulated as thoroughly as oil, but the metaphors (alternatives relate to water) as a combined force of nature to be tamed and resource to be exploited, evoking abundance, volatility and necessity while excluding humans (Puschmann & Burgess, 2014; Stark & Hoffmann, 2019). This has the further effect of reducing individuals to their expression as measurable data points. Hildebrandt builds on the suggestion that “not everything that can be counted counts, and not everything that counts can be counted (Cameron, 1963, p. 13), to suggest privacy as the “protection of the incomputable self” (Hildebrandt, 2019). Nakamura labels this a problem of cybertypes as “menu-driven identities” that reduce dynamic and expansive categories such as race or gender into minimal options in a “clickable box” that erases aspects of identity (2002, pp. 101-102). This is particularly the case for those between conventional normative identity markers, such as “the experiences of trans people [which] lay bare the limits of rigid or fixed data categories for capturing fluid or multifaceted identities” (Hoffmann, 2018a, p. 11). This highlights problems with empowering the multiple or networked self that Cohen (2012) elaborates,

as many are left no choice but to conform to (often incorrect) reductionist categories for access or representation.

Data as property to be possessed therefore raises the question of dispossession, as both the submission (subjection) of the subject to norms of recognition (in the performative construction of the subject) and the disowning or abjection of subjects by ideological norms (Butler & Athanasiou, 2013, pp. 1-2). Athanasiou highlights how "transgender suspends the certainties of having versus not having" (p. 55), calling into question the notion of gender (and here, by extension, any identity markers or data points) as property. The incomputable self, the self beyond menu-driven identities, the queer self, and the dispossessed self, call into question the very validity of identifying data beyond being a tool for political control. Pushing for equality in the application of privacy protections must entail an act of resistance towards the underlying system of measurement, production and capitalism that limits, for example, Zuboff's (2019) critique of surveillance and misuse of personal data. Without changing the power asymmetries of capitalism, corporations will always seek to mobilise new technologies for profit. Protecting individual data as property does little to combat these cultural dynamics.

Facebook has demonstrated this in court by attempting to argue that their users have "no expectation of privacy" (Thalen, 2019). This shows a conflation of two different expectations: being in public socially and having one's data exploited by a company. And yet the justification had already been used in a Canadian court against an individual claiming a breach of privacy (Zaman & Rudner, 2019). While concrete cases have thus far been only in specific scenarios (such as individuals being involved in employee group chats), Facebook itself clearly sees the principle as a general rule for their platform. This framework, based on data transferring to a platform as property, completely undermines privacy as freedom. Treating data as property entails treating users as products, an objectification of the population within corporate interests. In this system it is not only employees but users too who are considered *human resources*, with the customer now being other corporations seeking advertisement and influence.

We should also be wary of privacy as a branding exercise, and oppose the framing of privacy as a commodity (for the wealthy) that emerges from defining privacy as property. But even shifting ownership to users can fall into the protectionist dilemma. A report by the Open Data Institute recently concluded that "data is not capable of constituting property in the legal trust sense" (Reed et al., 2019, p. 12). This calls into question the legal basis of "data trusts" as collective alternatives to platform ownership of data, and raises further questions about considering privacy as property in a more general sense. Thinking in terms of property, and in particular its

protection, not only runs counter to net ideals of openness but also exacerbates existing inequalities. Understanding privacy in terms of protecting property can never be for everyone. Even within protectionist perspectives, framing privacy as property has limited effectiveness at best and acts as a method of commercialisation, exploitation, and control at worst.

Power

Beneath both freedom and property lies protecting privacy as the systemic protection of power in digital society. At first glance, and following the ideals of many involved in the early days of the internet, privacy displays a utopian relation to power. Privacy enables the creation of enclaves as alternative spaces, protected from oppressive political forces. These enclaves sustain a space in which alternative systems of power can emerge, a radical counter to the enclosure of citizens in digital spaces through privacy invasion (Andrejevic, 2009). In this sense privacy creates spaces for political desire, and protecting privacy becomes a source of empowerment. But entwined with informational power as control over access to knowledge/resources in digital society, privacy is part of the increasing "reality construction" by algorithmic governance (Just & Latzer, 2017). While privacy can act as a check on this use of data, as we have seen there are few legitimate protections that genuinely support groups and individuals marginalised by existing powers.

If technical tools are available, so the argument goes, the onus is on individuals having the power to protect their own privacy, leading to collective responsibility. But this focus risks inadvertently detracting from the responsibility of tech companies and governments, and is hardly fair on users considering the extent to which contemporary society is designed to manufacture participation at the expense of privacy. Emphasising the protection of power risks falling back on the complicity models prevalent in surveillance studies and privacy culture (Monahan, 2018). Privacy is not empowering if it involves exclusion from social reality, made worse by the uneven distribution of privacy and lack of other options for those from marginalised groups (such as the obstacles to privacy for those with certain disabilities).

Even keeping one's privacy, particularly as a marginalised group, can lead to exclusion by creating data gaps: facial recognition technologies with intersectional (mostly race and gender) inabilities to recognise faces (Buolamwini & Gebru, 2018; Keyes, 2018); or lack of sex-disaggregated data leading to a host of problems in health, work, safety, and representation (Criado-Perez, 2019). Even within poststructural forms of identity, we must remember that social relations are not always voluntary but form within the constraints of existing systems of meaning and power (Losh, 2015, p. 1651; Hoffmann, 2018a, p. 11). In light of this, if privacy is

a system of power it is one that will always, one way or the other, fail for the vast majority of the population.

Power exists asymmetrically in all aspects of society, and the ultimate power—power over who lives or dies (Mbembe, 2003, p. 11)—is therefore embedded throughout social relations. In defining this power of necropolitics, Mbembe asserts that “death and freedom are irrevocably interwoven” (p. 38), but also that death can take various material and social forms of violence and exclusion (whether bodily, access to income or severance from the rights and interactions of civil society). In this context, socially disengaged technologies do “more than simply reflecting problematic social attitudes, [they] reinforce and amplify them”, a systemic act of cultural and symbolic violence (Hoffmann, 2018b). This “data violence” is a digital form of institutional prejudice that is continually and acutely felt by already marginalised groups such as the trans and nonbinary communities. The iterative performance of this violence by governments and platforms exacerbates the normalisation of exploitative data practices and asymmetric systems of control around data use.

In a queer necropolitics, then, gender is pathologised in order to be erased, ostensibly to protect privacy—of, for example, the enforced suppression of pre-transition gender assignment in Iran (Shakhsari, 2014, p. 109)—while enacting a necropolitical power over marginalised communities through their quantification and exclusion. Butler warns that we must be wary of pathologisation in order for recognition (2015, p. 54)—particularly for trans people and the legal status of transition, and particularly when it is combined with an enforced act of erasure by external bureaucratic apparatus. This is a trend seen all too often in the discriminatory classification of characteristics in machine vision datasets that reduce individuals to perceived gender, racial, occupational, or health assignments. The necropolitics of personal data extends also into the afterlife, particularly for intersectional issues such as the appropriation of the identities of murdered trans persons of colour to serve dominant political rhetorics (Snorton & Haritaworn, 2013). The periperformative context of privacy should therefore extend beyond the removal of an individual from that context; integrity should be maintained regardless of whether an individual has moved, disengaged or died. Forward integrity, forward privacy is a collective periperformative duty.

Privacy can be used to both centralise and decentralise power. But the decentralisation of power does not itself mean better privacy or more power for individuals. Deleuze (1992) defines the society of control in terms of access to data, and Galloway (2004) builds on this to suggest protocols as the method of managing a decentralised control-based society. Current calls for regulation of big tech show how this has played out in practice, with companies able to amass power through the

decentralised networks of the internet. These new powers not only operate as loci of globalised wealth, but as controllers of access to platforms and services that form informational (and thereby social) reality. Privacy is not equal to power, but it is synonymous with how it operates in control society, and provides a good indicator of where power lies, highlighting existing inequalities and the commodification of power as the purview of privilege. Protecting protocological power (which, as access and control, runs parallel to privacy) does little for the individual as decentralised systems generate new forms of oppression and exploitation, a seeming drive towards global community underpinned by a "manifesto" of access to personal data that condemns users to engage (Rider & Wood, 2018). Corporate rhetorics of privacy—in both policies and marketing—can be seen primarily as tools of mass disempowerment.

A protectionist standpoint makes it difficult to move on from thinking in terms of *power over*, even so far as having power over one's data. Instead, privacy can be better thought of as empowerment—*power to* and *power with*—both individually and collectively. This framing leads towards a more performative and collaborative approach, and positions privacy as a means of protecting other rights, such as freedom of assembly (Privacy International, 2019). But protections around privacy also give platforms "the capacity to disempower [users] at will" (Schwarz, 2019, p. 136). This disempowerment also occurs at a systemic and structural level, with the manipulation of consent through the increasing need to use data-collecting platforms to access key networks for health, education, social, and other needs. Noble (2016) highlights the need for intersectional critique of the way "technological ecosystems" structure "detrimental narratives" in service of "material disenfranchisement," echoed by Hoffmann (2018a) in the need to overcome the separation of different characteristics when considering marginalisation and the impossibility of "uncomplicated claims to neutrality or objectivity" (p. 7). The protectionist view, as a reductionist and therefore contextually limited effort always doomed to fail, enacts a sense of resignation cultivated by corporate power (Draper & Turow, 2019). This discussion has outlined how a protectionist approach to privacy therefore concedes a continual losing battle for many individuals. To reposition privacy as a positive force, and even to "protect" it, we need alternative frameworks that inspire collective equality, equity, and action.

Performing privacy

The concept of performativity from gender theory provides a useful framework to critique protectionist constructions of privacy and generate positive collective performance (and thereby societal identity construction) of privacy beyond and against the failed liberal idea of the Enlightenment individual subject. Queer performative sociology allows us to broaden "an

understanding of power to include identity formations as well as other discursive formations" and "treating the construction of intersectional subjectivities as both performed and performative" (Valocchi, 2005, p. 766). This approach promotes diversity and equality through emphasising action and process rather than a state that obtains (to use legal terminology) or needs protecting. Butler's (1988) conception of performativity is instructive in critiquing and mobilising the individual-collective relation of creating and entrenching constructed norms and roles around which privacy and power accumulate.

The first step of performative privacy is emphasising the link between individual and collective structures. As Butler writes:

> The personal is thus implicitly political inasmuch as it is conditioned by shared social structures, but the personal has also been immunized against political challenge to the extent that public/private distinctions endure. (Butler, 1988, pp. 522–3)

Privacy is often thought of as protecting the individual, but in so doing it is always already political and collective, part of a constructed social relation of access/control based on the fundamental division of self and other (Altman, 1975, p. 50, 1977, p. 67). Petronio (2002) attempts to push this further by taking a more metaphorical and dynamic approach, but remains focused on the construction of boundaries as the definition of the self. A critical performative perspective therefore begins by challenging this assumption, removing the public/private divide and envisioning privacy in terms of a relational and contextual identity that is performed together. Privacy does not disappear in public, it is performed in, through and with publics and public spaces. Sedgwick (2003, p. 75) builds on Butler and follows Derrida with thinking the performative as being self-referential based in a historical (past and future) force beyond itself, but adds that we must also consider the *periperformative*, an alloreferential occurring temporally around a performative act to affirm or challenge it. The periperformative is the context of a performative act—its social-relational metadata—and the collective contribution to the performative utterance. In the terms of Nissenbaum's contextual integrity, the norms of privacy are performative while contexts are periperformative.

A periperformative framing highlights the blurred boundary between the individual, group or abstract entity, bridging personal and political narratives. Periperformatives therefore "*allude* to explicit performative utterances," they describe or even negate the performative, they are "*about* performatives" rather than being an act in themselves, "they cluster around them" but with "no very fixed circumference" (Sedgwick, 2003, p. 68). Periperformatives acknowledge the assumed 'they' bearing witness to a performative act, the collective component of privacy that situates and supports an individual's agency through collective enforcement. This can

be used positively or negatively, to reinforce unequal power structures or to enact radical change.

Performativity was used by Butler to critique social and individual repetitions of fixed roles and identities, and this self-referential feedback loop of identification and subjectification (notably in gender but also in the wider categorisation of individuals as data) is difficult to escape. In this context, the legal protections of the liberal self appear as one (narrow and often negative) performance of perpetuating roles and constraining contexts that fix individuals into prescribed norms, against which a gender approach would require performative acts of resistance that emphasises the fluid incomputable aspects of the poststructural self. Sedgwick writes that the performative context, like a play, is "constituted as a spectacle that denies its audience the ability either to look away from it or equally to intervene in it" (2003, p. 72), and that "to disinterpellate from a performative scene will usually require, not another explicit performative nor simply the negative of one, but the nonce, referential act of a periperformative" (p. 70). Overcoming performative repetition of inequalities through critical periperformative disinterpellation of their power structures and social contexts is therefore a necessary step towards collectively performing privacy as the act of looking away, of refusing to accept, engage in or bear witness to forced access to or exploitation of data, even if that data is performed in public. What this means is using collective contexts to challenge the normalisation of exploitation and power inequality, removing the fear and risk from being in public (a problem that goes well beyond privacy). It is a collective act of respect that looks away.

This is a key issue of social media: the need to individually choose and collectively support different audiences for different utterances without the exploitation of corporate or state technical-legal systems that entrench existing power structures. We must subvert and reappropriate the compulsory witness of social constructs. This entails challenging the assumption that a lack of privacy, for example, has become an unavoidable part of life in networked society. It is a challenge to the systemic forcing of participation in privacy-invasive platforms and socioeconomic structures. For example, it is refusing to share privacy-invasive or hateful material online—or, better yet, refusing to watch or read such material in the first place. We must shift from complicity in fear-based (self-)victimisation to collective performance of privacy as a positive social construct when combined with the periperformative disinterpellation of contextual integrity as an inherent part of the metadata of a speech act, whether online or offline. In an age where metadata and our networks or connections can undermine privacy even if the individual themselves is apparently protected, we need to build new forms of trust in societal

systems (Kerry, 2018), and in the integrity of social contexts, in order to undertake collective action and empowerment.

Identity

Beyond the reductionism of control-based society that breaks up users into static data points—the process of *dividuation* that converts individuals into *dividuals* (Deleuze, 1992) which "are then governed automatically through databases and levels of access and exclusion" (Whitson, 2015, p. 343)—we must push further into the fluidity of the self, past structural regulation and into poststructural and relational debates as critiques of subjects, information, and power in order to perform privacy. Thinking of privacy in terms of identity is a useful framework for bridging individual and collective acts and perspectives, as it can be used to emphasise diversity—particularly the intersectional and context-specific concerns around the implications or empowerment of privacy—and indeed to support existing rights-based protections of privacy. It also extends, for example, Nissenbaum's focus on appropriate flow of *information* to include, for example, bodily privacy or cyberphysical public spaces. These are important areas for intersectional issues in privacy and the complex relations between physical and digital identities.

Identity stands against privacy as property. Floridi (2015a) suggests that we should let go of thinking about personal data in terms of the philosophy of economics (the property-based framework of surveillance capitalism), stop legislating in terms of ownership of data as a 'thing', and move towards thinking personal data in terms of the philosophy of mind. In this framing, *my data* is "mine because they constitute me" (Floridi, 2015a). Privacy invasions are therefore less about trespassing (imposing on another's property) and more akin to kidnapping (taking another's self). This maintains the privacy of personal information or memories even when they are acquired in a public place, for as Floridi points out, "kidnapping is illegal even in public spaces" (2015a). He pushes this view further in relation to the philosophy of memory, emphasising the right to be forgotten (which he insists is an unhelpful name) as being about managing, or 'closing', memory:

> dealing with closure has become difficult on the web, a flatland lacking historical depth. [...] We must ensure that the right kind of personal information may be remembered (no removal of past information) without being constantly recalled (no unnecessary resurfacing of past information). (Floridi, 2015b, p. 43)

This temporal closure—the act of "remembering without recalling"—can be understood as a collective act of periperforming the fact of remembering without actually performing the recalling. It acknowledges the relationality of access to information and supports social connections, while maintaining an individual's ability to control the temporal context of their utterances.

The ahistorical entrenchment of data as a flat ontology presents a barrier to radical performativity. It is therefore important to think of the self not as singular or fixed but as fluid: “an identity tenuously constituted in time—an identity instituted through a *stylized repetition of acts*” (Butler, 1988, p. 519). At first glance, data appears to run counter to performativity and to privacy, abstracting identity into dividual units of categorisation that stick inescapably with an individual across their various online interactions. But if we think with Butler that identity is always a stylisation, we can reinsert performance into data to challenge how it is operationalised by surveillance (state or capitalist) systems. If we understand that data is only ever a snapshot of one particular expression in one particular moment, we can begin to establish a framework for supporting privacy through time.

Identity here is always plural, identified by Green in the long sociological tradition of treating the self and identity as multiple and fluid (2007, pp. 27-8), working alongside and in tension with queer theory as “a radical anti-identity politics [that] rejects a stable, knowable subject” (p. 29). We must therefore insert a separation, a “performative interval” which “marks the distance between doing and identity whereby the doing (e.g., doing woman) represents practice and identity (e.g., female) an interior semblance of self” (p. 32). Data and identities are both only ever a semblance, a representation, and interpretation. They are always relational and always suggest a separation from the individual as they appear within the performative context.

Butler insists that we must “understand constituting acts not only as constituting the identity of the actor, but as constituting that identity as a compelling illusion, an object of *belief*” (1988, p. 520). Within any given performative context (work, family, social media, gaming) we collectively agree to the periperformative framework within which we sustain the illusion of fixed measurable identity. But if, as Butler follows de Beauvoir in the idea that one is never born but only becomes a woman, we assert that facticity (and its expression in data) is separate from cultural meaning, then we can start to mobilise this belief for productive performative ends. And is all of cyberspace not, as a cultural representation of networks and data, a “consensual hallucination” (Gibson, 1995 [1984], p. 67)? If so, it can be created to represent corporate or state interests, or recreated as a new stage in which the collective belief in privacy empowers users together. We *become* categories of data, and can do so as a critical operation in which we also become otherwise, performing across categories as we perform different (parts of our) identities.

Beneath the performance of identification, dissolution and fuzzy boundaries that constitute our identities—into the importance of the uncountable and incomputable (Hildebrandt, 2019)—we must therefore

always include the performative interval between data and self as part of a periperformative social and spatiotemporal context, separating our fluid inner selves from their countable utterance as data. Athanasiou emphasises recognition and the act of revealing as important for trans people in particular (Butler & Athanasiou, 2013, p. 56). This shows the entwined nature of sharing and keeping secret within privacy, and the periperformative aspect of the appropriateness of information flow, use and response. This is a profoundly political project that acknowledges and attempts to overcome the forcing of quantified identities on individuals through excessive categorisation by indifferent or malicious institutions.

Performing identity as privacy means being heard. It is therefore also a struggle against "data violence" (Hoffmann, 2018b) and the systems of power that convert performed identity into subjectification and oppression. Performing privacy as identity includes our online interactions that occur outside our usual ontologies: asynchronous, multiple, and apparently immaterial. It is thus through the act of performing identity (whether countable, uncountable, or relational) that we are embodied less in data than in metadata. Identities are always implied, always speculative, as they emerge from what is left out of data but suggested through metadata. It is therefore important to perform identity as a limit of the dissolution of the self, constantly recreated in the social contexts of specific relations of access and control, or privacy. Performing privacy invites us to embrace the uncountable, the fluid, and the multiple in our construction of identity. Performing privacy empowers greater ability to perform the self.

Consent

Alongside identity, it is fitting in thinking privacy as a performative process to consider consent as a driving framework for determining social relations. Consent has been a core component of queer privacy (Lewis, 2017, p. 1), emphasising the everyday struggles of marginalised groups as well as the blurred boundaries between the many different intersecting populations that form global digital society. For Lewis, privacy requires understanding of different needs, including the different contexts in which one might want or need privacy, and that this in turn requires diverse voices in the debate: "nothing about us, without us" (p. 2). This includes the role of privacy in issues of domestic abuse, workplace or public prejudice, online dating and connected sex, as well as an integral aspect of sharing. Privacy as contextual integrity overcomes the constraining conception of access control as a limiting, secretive and protectionist process.

Privacy always includes sharing, as long as it respects the consent of the relational network involved in the act of sharing and the information shared. While this must always be understood temporally (it is consent during or for a specific interaction, but also incorporates privacy in memory

and the right to be forgotten), taking a performative approach to the issue is thereby a better support even for freedom, property, and power than a protectionist framework. If we perform openness, we can enable transparency, accountability, and access to necessary information. But this is part of the same performance that collectively negotiates trust over the use of information. An example is access to sexual health advice. This is necessary for individuals, particularly women (and even more specifically, younger women or those from communities in which such advice may not always be available as a matter of course), in order to enable their autonomy and support their self-development. But the metadata surrounding this exchange of information (whether it is the contents of any discussions or the very fact of searching online for advice) should remain private, to enable informed autonomy and the construction of a supportive community. As Altman suggests, autonomy must be extended to the "social psychological process" of regulating interpersonal contact (1977, pp. 69, 83). But this too must be extended into the creation of collective contexts and maintaining the integrity of such social relations, in order to reach a notion of privacy beyond separation.

The broader context is also important as part of this relational act of privacy, including issues of age, assault or abuse, termination, and other aspects that may require a performative and periperformative blurring of privacy to ensure relevant accountability and support without victimising the person seeking advice. In this example, privacy is collectively performed in the act of making public a request for advice (whether directly to another human and/or through digital platforms to connect the individual with the most appropriate resources) which is then collectively made private through the shifting of a periperformative context around the act (i.e. no information is stored or shared unless consented is actively given). In this sense, periperformativity can be considered also as the *metadata* of privacy, the always-there third-person utterance "about" the exchange (or not) of information that defines its collective privacy.

It is certainly true that existing consent mechanisms are inadequate, particularly the "transparency and choice" or "notice and consent" models that have come under intense criticism (Nissenbaum, 2011, pp. 34-36). Even after steps such as GDPR, this corporately co-opted framework has failed to provide individuals with adequate transparency and genuine choice, consent as a concept forms a basis upon which to establish the specific contexts around which integrity would form. For Nissenbaum, it is the very concept of consent that is inadequate. We argue instead that offering true consent—rather than forcing it—can be viewed as a performative act that frames a context by an individual in conjunction with the socially periperformative context within which the information flow will operate. We can again return to the need to consider embodied experiences of marginalised groups and reassess how we can use

consent as an active performative framework. However, there are warnings against the potential trivialisation of sex ethics as a metaphor for data ethics (Stark & Hoffmann, 2019). Therefore, in leaning on consent here, we do not wish to sexualise technology, which is often used as an exclusionary tactic to prop up gender and racial power structures. Instead we aim to highlight how sex and gender (and bodies more broadly) must be taken into account within privacy. Doxing, revenge porn, online sexual threats, stalkerware and biometric data are very real concerns that show how the task of creating constructive periperformative privacy contexts must always be made in connection to existing drives towards inclusive and sensitive models of consent and identity.

Consent is no mere metaphor but part of an interconnected and intersectional web of material, social, cultural and affective respect. Models such as the "consentful tech" project (Lee & Toliver, 2017)—which promotes consent as freely given, reversible, informed, enthusiastic and specific - can offer practical methods of performing privacy. Consent therefore moves towards Hoffmann's call for a design culture of "support and resources" without judgement, based in "empathy and thoughtfulness" (2018b). Privacy as consent requires a periperformative context of respect that resists enforced participation and offers a genuine choice, genuine agency for individuals and collectives to perform without exploitation. If consent has failed in practice, it is because it has been built on protectionist notions and relegated to a *condition* of data use (and thereby misuse). Consent should form an underlying principle of privacy, an inherent part of the context of information. Privacy-respecting standards, models or presets (assuming no access rather than manipulating conditions for access) might offer one way of enabling a (peri)performative roles and relations in managing the appropriate flow of information.

Rather than rights, which in privacy will invariably fall back on defensive terminology, consent shifts the emphasis from power over and even power to, which hits a protectionist limit even as a 'positive' right, towards a negotiation of the boundaries between *power with* and *power within* (Veneklassen & Miller, 2002, p. 55), the need for self-knowledge, respecting difference, and building solidarity for social transformation. As a performance of consent at the blurred, relational boundary between individuals or entities, power with forms the sharing of information (always in a specific and limitable spatiotemporal context) while power within occurs at the empowerment of control by the individual to recall consent at any time. This sharing and resituating of power in and between individuals grounds collective privacy as a mutual performance based on consent and respect, and its links to existing sexual politics, regulation and legal recourse provide a concrete framework for supporting and ensuring this empowerment without resting on protectionist language.

Comparisons are often made between Bentham and Foucault's panopticon and surveillance mechanisms embedded in online society. But these have become increasingly problematic. Tufekci (2014), among others, have shown that where the panopticon functions as a constantly visible possibility of surveillance, digital surveillance is an invisible constant certainty. But (as Tufekci suggested may happen in the wake of the Snowden revelations) the situation is more complex and indeed more performative. Users are aware of and concerned about the risks to their privacy, but this is not often embodied in their behaviour. This is the privacy paradox in which users know that they most certainly are being constantly monitored, but act as if that is not the case (Black et al., 2018), an oppressive social performance that underlines digital surveillance society. Digital surveillance has become simultaneously visible and invisible.

Power in such a structure exists everywhere and nowhere, coalescing around those who control the platforms and network infrastructure. In such a society of control (Deleuze, 1992) or protocol (Galloway, 2004), there is a fundamental barrier to true consent as access is not only limited but also to a certain extent enforced in order to engage with social reality in digital society. Critical performative interventions are required to challenge this self-perpetuating illusion of choice. If “the performance renders social laws explicit” (Butler, 1988, p. 526), then we must collectively adjust our periperformative context in order to refuse the current system. If performative reality “is real only to the extent that it is performed” (p. 527), then it can also be performed otherwise. There is an urgent need to address these issues of consent in our escalating data-driven, cyberphysical, algorithmically governed, ‘smart’ society.

Fear-based privacy has failed large swathes of the population, and a more positive, collective model is required. A report by the Our Data Bodies project on data collection in major urban areas in the US found that citizens have a desire for “power not paranoia” (Petty et al., 2018, p. 19) and “want to be seen, not watched, and heard, not harmed” (p. 22). This notion echoes Chun’s call for the means of being in public without being exploited (2016). Consent-based performative privacy moves towards achieving this aim, using the theatrical component to performative acts that designate a specific stage or arena in which acts occur and consequently in which the corresponding social structures emerge (Butler, 1988, p. 527). Consent is required by both the actor(s) and audience(s), but should also be considered ongoing in memory (biological and technical), with consent (and its conditions such as the level of attribution or anonymisation) being able to be withdrawn at any time. This goes well beyond specific legal methods of withdrawal, such as the problematic Right to be Forgotten, into the very structure of information society. Privacy as consent is a complex, global, spatiotemporal relation of

information flow that forms social bonds through collective respect of the performative acts and the periperformative contexts in which they are situated.

Action

The performative act is “both that which constitutes meaning and that through which meaning is performed or enacted” (Butler, 1988, p. 521), not a matter of *expressing* (which suggests prior existing categories) but of *doing* (p. 528). Green suggests that “queer theory focuses on the performative failure—that is, the inability of the individual to fully realize the concept and lay claim to ontological status” (2007, p. 32). In other words, privacy is about *becoming*, not being. This is a critical-creative process building on two concepts of performance. The performative action is an introverted deconstructive speech act but is also at the same time an extroverted theatrical act (Sedgwick, 2003, p. 7). In this sense, performing privacy is a matter of agency over the division, signification and display of (parts of) our identities and our social realities.

Butler (1988) writes of the performative as a “constituted *social temporality*” (p. 520) with possibilities for cultural transformation, formed of the acts of individuals, taken together, which can perform radical acts which question the existing structure and can thereby constitute new social structures (p. 523), through the power of subversive performances that can change the cultural field (p. 531). This is the focus of Skinner-Thompson’s performative analysis of “anti-surveillance camouflage” that frames privacy “less as defensive efforts for secrecy, and more as affirmative acts of expression” (2017, p. 1734). These techniques (including masks, makeup or clothing) build on privacy as integral to identity. However, they also risk merely enacting “an aestheticization of resistance premised on individual avoidance rather than meaningful challenge to the violent and discriminatory logics of surveillance societies” (Monahan, 2015, p. 159). The performative challenge to existing power structures requires a periperformative desire (Sedgwick, 2003, p. 74) for collective action beyond the individual act. The periperformative can also “dramatize the pathos of uncertain agency, rather than occluding it as the explicit performative almost must” (p. 76). Between the performative and the periperformative, the act and its context(s), is a negotiation of the grey areas, an embracing of the diversity and even difficulty of constituting positive collective action.

Nissenbaum attempts to demarcate separate spheres of influence for law, politics and social norms (2004, pp. 156–157). This is surprising given her emphasis on the complexities of different public/private spheres beyond clear-cut divisions. Similarly, her assertion that abortion should be a component of a full theory of privacy (which indeed it should), sits against her exclusion of "courtship" from regulation (victims of abuse, sexual

assault, or rape would beg to differ). She also places the political as only relevant in extreme cases of violation, which again seems entirely unsatisfactory to feminist and gender perspectives. While avoiding the legal default to regulation as a solution, Nissenbaum fails to fully integrate policy within politics and society. These combined methods should be considered within any given context. This is perhaps why Nissenbaum's contextual integrity has preference for status quo (2004, pp. 144–145). As existing contexts are never neutral and almost never equal, this is a worrying starting point. While acknowledging justified change, there is the question of influence over norms (particularly when considering the often-biased positions of mainstream legal and political institutions), and the entrenching of particular already dominant interests. A performative approach, by contrast, acknowledges the perpetuation of social norms (in a way that is sensitive to both prescriptive and descriptive definitions) but also provides a means for bottom-up change, representation for marginalised groups, and a challenge not only to the status quo but the systems of power that define and maintain the status quo.

The first step towards privacy as social action is to generate more positive and more productive information cultures. Like identity, culture is always plural here, for there are diverse and intersectional perspectives to take into account when designing systems that support the privacy requirements of all users. Generating new cultures occupies Butler's call to action: "to do, to dramatise, to reproduce", to embody in the "materialising of possibilities" as a dramatic act (1988, p. 521). But in creating these new meanings there is also the need for "articulating periperformative choices that create highly charged thresholds of meaning" (Sedgwick, 2003, p. 82) to challenge asymmetries in agency. We can thereby create the context in which more positive acts/social structures can be performed. Lewis asserts that "Queer Privacy is about building tools to destabilize and destroy the status quo" (2017, p. 3), echoing Sedgwick's push for moving beyond the exemplary (2003, p. 79) by creating not single examples but a framework of tools and practices for constant critical creation of new social norms, an approach suited to the nuances of cultural diversity and specificity of marginalised groups.

Performing privacy in action is to critique existing structures of data collection and exploitation with new utterances of identity and consent in socio-relational networks built on choice, agency, and respect. Performativity as a collective act stands from and against precarity—not identity—as the "rubric" that brings together intersectional marginalised groups (Butler, 2015, p. 58). As Murakami Wood writes, "the more precarious one's conditions of existence and one's class, racial, gender—and so on—identity, the more that such markers become identifications, the result of processes of control, and less identities, the product of self-definition" (2017, p. 45). Performing identity and privacy (including

sharing) together as a collective act of resistance therefore undermines the limited and discriminatory implications thrown up by thinking in terms of rights and property. It is, then, not identi*fication* but (embodied or, perhaps rather, embedded) presence that forms the collective identity of resistance and the performative identity as part of such collective resistance. This is about removing restrictions on the ability of an individual or group to make a performative utterance and define the context of such an utterance, the enabling of a position from which to speak (or not). It is the creation of a space for action by creating a space in which information norms can be questioned. This includes overcoming menu-driven collection and quantified identities in favour of more narrative, relational, and culturally embedded forms of collecting, storing, and using data. It is a matter of social justice, therefore, to, for example, replace limited dropdown menus of characteristics with qualitative and narrative options. This is particularly the case for gender, which if necessary should be an open text box rather than any given set of prescribed options.

Better yet would be to develop temporally flexible approaches alongside a constant questioning of whether any particular item of data should even be collected in the first place. Useful here is Glissant's (1997) mobilisation of opacity as a force which protects the Diverse, against "reductive transparency" (p. 62). It is the "real foundation of the Relation, in freedoms" (p. 190), the basis for solidarity with the Other (p. 193), and upon which transparency is imagined as part of a relation (p. 192). Blas (2014, 2016) further expands this concept as a basis for contemporary feminist and queer politics and aesthetics against the context and assumption of total surveillance, a resistance to the normalising and categorising expectations of intrusive and exclusionary social interaction. Beyond this critique, privacy as action is the creative process of generating new positive periperformative contexts through collected individual speech acts that expect and respect privacy.

Conclusion

This article has presented an alternative to current protectionist conceptions of privacy by critiquing the prevailing and often fear-inducing definitions of privacy, as is seen across science, engineering, law, press, and media. Protectionist measures, taking privacy as access and control, are all too often co-opted by corporate and state actors in the society of control, leading to helplessness on the part of users and citizens. Highlighting the inherent difficulties in protecting privacy in relation to traditional debates of freedom, property, and power, a new way of thinking privacy has been proposed. In order to support privacy as an empowering force for equality, diversity, and inclusivity, an outline for performing

privacy has been detailed, building on gender theory and applying it to identity, consent, and action as key components of building positive cultures of privacy.

But privacy never occurs in isolation. Issues of performing identity and consent in data are deeply embedded in our socio-technical relations. Most obviously with data science, but in the society of control this leads directly on to algorithmic decision-making, whether for content filters, targeted advertising, access to healthcare or the ethics of self-driving cars. Thus a related application of the framing of privacy presented here would be useful in, for example, performing artificial intelligence as a collective endeavour of trust and responsibility. We can also look to further theories that would inform the ongoing debate and development, such as Haraway's "informatics of domination […] as a massive intensification of insecurity and cultural impoverishment" (1991, p. 172) as well as her situated knowledges and critique of partiality (1988), or Braidotti's (2013, p. 38f) critical posthumanism as a relational conception of humans with blurred boundaries that overlap with ecological and technological environments. Practical creative acts of performing privacy can also be seen emerging in the Deep Lab collective supporting fluidity through "multi-pseudonymous identity" (Wagenknecht, 2014, p. 12), Gibson's crypto-choreography and the performing of encryption (2018) or Blas's collective queering of facial recognition and surveillance (in the works *Facial Cages*, *Facial Weaponisation Suite* and *Contra-Internet* which move beyond individual protection into a collective performance of identity as privacy). Performing privacy offers a mode of thinking that supports positive acts by individual users as part of a collective effort to create alternative social structures in which privacy can become an integral part of digital communication and social relations.

References

Altman, I. (1975). *The environment and social behavior: Privacy, personal space, territory and crowding.* Brooks/Cole.

Altman, I. (1977). Privacy regulation: Culturally universal or culturally specific? *Journal of Social Sciences, 33*(3), 66–84.

Andrejevic, M. (2009). Privacy, exploitation, and the digital enclosure. *Amsterdam L.F. 1*, 47–62.

Bamberger, K. & Mulligan, D. (2011). Privacy on the books and on the ground. *Stanford Law Review, 63*(2), 247–316.

Black, C., Setterfield, L. & Warren, R. (2018). Online data privacy from attitudes to action: An evidence review. *Carnegie UK Trust*. https://www.carnegieuktrust.org.uk/publications/data-privacy-from-attitudes-to-action/.

Blas, Z. (2014). Informatic opacity. *The Journal of Aesthetics and Protest, 9*.

Blas, Z. (2016). Opacities: An introduction. *Camera Obscura, 31*(2), 149–153.

Blum-Dumontet, E. (2019). "Betrayed by an app she had never heard of"—How TrueCaller is endangering journalists. *Privacy International*. https://privacyinternational.org/case-study/2997/betrayed-app-she-had-never-heard-how-truecaller-endangering-journalists

Braidotti, R. (2013). *The posthuman*. Polity.

Browne, S. (2015). *Dark matters: On the surveillance of blackness*. Duke University Press.

Buolamwini, J. & Gebru, T, (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. *Proceedings of Machine Learning Research, 81*, 1–15.

Butler, J. (1988). Performative acts and gender constitution: An essay in phenomenology and feminist theory. *Theatre Journal, 40*(4), 519–531.

Butler, J. (2015). *Notes toward a performative theory of assembly*. Harvard University Press.

Butler, J. & Athanasiou, A. (2013). *Dispossession: The performative in the political*. John Wiley & Sons.

Cameron, W. (1963). *Informal sociology: a casual introduction to sociological thinking*. Random House.

Children's Commissioner for England. (2018). Who knows what about me? *Children's Commissioner*. https://www.childrenscommissioner.gov.uk/our-work/digital/who-knows-what-about-me/

Chun, W. (2016). *Updating to remain the same: Habitual new media*. MIT Press.

Cohen, J. (2008). Privacy, visibility, transparency, and exposure. *University of Chicago Law Review, 75*, 181–201.

Cohen, J. (2012). *Configuring the networked self: Law, code, and the play of everyday practice*. Yale University Press.

Cohen, J. (2013). What is privacy for? *Harvard Law Review, 126*(7), 1904–1933.

Criado-Perez, C. (2019). *Invisible women: Exposing data bias in a world designed for men*. Vintage.

Delacroix, S. & Lawrence, N. (2018 [revised 2019]). Disturbing the 'one size fits all' approach to data governance: Bottom-up data trusts. *SSRN*. https://dx.doi.org/10.2139/ssrn.3265315

Deleuze, G. (1992). Postscript on the societies of control. *October, 59*, 3–7.

Draper, N. & Turow, J. (2019). The corporate cultivation of digital resignation. *New Media & Society*.

Dwork, C. & Mulligan, D. (2013). It's not privacy, and it's not fair. *Stanford Law Review, 66*, 35–40.

Floridi, L. (2015a). On personal data, forgiveness, and the "right to be forgotten." *Markkula Center for Applied Ethics*. https://www.youtube.com/watch?v=JVTu-0SfvzQ.

Floridi, L. (2015b). "The right to be forgotten": A philosophical view. *Jahrbuch für Recht und Ethik-Annual Review of Law and Ethics, 23*(1), 30–45.

Galloway, A. (2004). *Protocol: How control exists after decentralization*. MIT Press.

Gibson, R. (2018). Crypto choreography/soma spy. In *A World of Muscle, Bone & Organs: Research and Scholarship in Dance* (408-433). C-DaRE.

Gibson, W. (1995 [1984]). *Neuromancer*. Voyager.

Glissant, É. (1997). *Poetics of relation*. University of Michigan Press.

Green, A. (2007). Queer theory and sociology: Locating the subject and the self in sexuality studies. *Sociological Theory, 25*(1), 26–45.

Greenberg, A. (2019). Hacker Eva Galperin has a plan to eradicate stalkerware. *Wired*. https://www.wired.com/story/eva-galperin-stalkerware-kaspersky-antivirus/

Haraway, D. (1988). Situated knowledges: The science question in feminism and the privilege of partial perspective. *Feminist Studies, 14*(3), 575–599.

Haraway, D. (1991). A cyborg manifesto: Science, technology, and socialist-feminism in the late twentieth century. In *Simians, Cyborgs and Women: The Reinvention of Nature* (149–181). Routledge.

Hildebrandt, M. (2019). Privacy as protection of the incomputable self: From agnostic to agonistic machine learning. *Theoretical Inquiries in Law, 20*(1), 83–121.

Hill, J.L. (2004). The Five Faces of Freedom in American Political and Constitutional Thought. *Boston College Law Review, 45*, 499-594.

Hoffmann, A. L. (2018a). Data, technology and gender: Thinking about (and from) trans lives. In J.C. Pitt and A. Shew (Eds.), *Spaces for the future: A companion to philosophy of technology* (3–13). Routledge.

Hoffmann, A. L. (2019). Where fairness fails: Data, algorithms, and the limits of antidiscrimination discourse. *Information, Communication and Society, 22*(7), 900–915.

Hoffmann, A. L. (2018b). Data violence and how bad engineering choices can damage society. *Medium*. https://medium.com/s/story/data-violence-and-how-bad-engineering-choices-can-damage-society-39e44150e1d4

Horvitz, E. & Mulligan, D. (2015). Data, privacy, and the greater good. *Science, 349*(6245), 253–255.

Igo, S. (2015). The beginnings of the end of privacy. *The Hedgehog Review, 17*(1), 18–30.

Igo, S. (2018a). Me and my data. *Historical Studies in the Natural Sciences, 48*(5), 616–626.

Igo, S. (2018b). *The known citizen: A history of privacy in modern america*. Harvard University Press.

Just, N. & Latzer, M. (2017). Governance by algorithms: Reality construction by algorithmic selection on the Internet. *Media, Culture and Society, 39*(2), 238–258.

Kerry, C. (2018). Why protecting privacy is a losing game today—and how to change the game. *Brookings Institute*. https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/

Keyes, O. (2018). The misgendering machines: Trans/HCI implications of automatic gender recognition. *Proceedings of the ACM on Human-Computer Interaction, 2*(CSCW), 88.

Lee, U. & Tolliver, D. (2017). Building consentful tech. *Consentful Tech*. http://www.consentfultech.io/

Lewis, S.J. (2017). *Queer privacy: Essays from the margins of society*. Mascherari.

Losh, E. (2015). Feminism reads big data: “Social physics,” atomism, and Selfiecity. *International Journal of Communications, 9*, 1647–1659.

Mamonov, S. & Koufaris, M. (2016). The impact of exposure to news about electronic government surveillance on concerns about government intrusion, privacy self-efficacy, and privacy protective behavior. *Journal of Information Privacy and Security, 12*(2), 56–67.

Mbembe, A. (2003). Necropolitics. *Public Culture, 15*(1), 11–40.

Mills, J. (2008). *Privacy: The lost right*. Oxford University Press.

Monahan, T. (2015). The right to hide? Anti-surveillance camouflage and the aestheticization of resistance. *Communication and Critical/Cultural Studies, 12*(2), 159–178.

Monahan, T. (2018). Ways of being seen: Surveillance art and the interpellation of viewing subjects. *Cultural Studies, 32*(4), 560–581.

Mokrosinska. D. (2018). Why states have no right to privacy, but may be entitled to secrecy: A non-consequentialist defense of state secrecy. *Critical Review of International Social & Political Philosophy*, 1–30.

Nakamura, L. (2002). *Cybertypes: Race, ethnicity, and identity on the internet*. Routledge.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review, 79*(1), 119–158.

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

Nissenbaum, H. (2011). A contextual approach to privacy online. *Daedelus, 140*(4), 32–48.

Noble, S. (2016). A future for intersectional black feminist technology studies. *Scholar & Feminist Online, 13*(3), 1–8.

O'Callaghan, P. (2012). *Refining privacy in tort law*. Springer.

Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure*. State University of New York Press.

Petty, T., Saba, M., Lewis, T., Gangadharan, S.P. & Eubanks, V. (2018). *Reclaiming our data: Interim report*. Our Data Bodies.

Puschmann, C. & Burgess, J. (2014). Big data, big questions: Metaphors of big data. *International Journal of Communication, 8,* 1690–1709.

Reed, C., BPE Solicitors, & Pinsent Masons. (2019). *Data trusts: Legal and governance considerations*. Open Data Institute.

Rider, K. & Wood, D. M. (2018). Condemned to connection? Network communitarianism in Mark Zuckerberg's "Facebook manifesto". *New Media & Society, 21*(3), 639–654.

Rød, E. & Weidmann, N. (2015). Empowering activists or autocrats? The internet in authoritarian regimes. *Journal of Peace Research, 52*(3), 338–351.

Schwarz, O. (2019). Facebook rules: Structures of governance in digital capitalism and the control of generalized social capital. *Theory, Culture & Society, 36*(4), 117–141.

Sedgwick, E. (2003). *Touching feeling: Affect, pedagogy, performativity*. Duke University Press.

Shakhsari, S. (2014). Killing me softly with your rights: Queer death and the politics of rightful killing. In J. Haritaworn, A. Kuntsman, & S. Posocco (Eds.), *Queer necropolitics* (93–110). Routledge.

Skinner-Thompson, S. (2017). Performative privacy. *U.C. Davis Law Review, 50*(4), 1673–1740.

Snorton, R. & Haritaworn, J. (2013). Trans necropolitics. In A. Aizura& S. Stryker (Eds.), *Transgender studies reader, Vol. II* (66–76). Routledge.

Solove, D. (2005). A taxonomy of privacy. *University of Pennsylvania Law Review, 154*(3), 477–564.

Solove, D. (2008). *Understanding privacy*. Harvard University Press.

Stark, L. & Hoffmann, A. L. (2019). Data is the new what? Popular metaphors & professional ethics in emerging data culture. *Journal of Cultural Analytics*.

Thalen, M. (2019). Facebook lawyer says users 'have no expectation of privacy'. *Daily Dot*. https://www.dailydot.com/debug/facebook-lawyer-no-expectation-of-privacy/.

Tufekci, Z. (2014). Engineering the public: Big data, surveillance and computational politics. *First Monday, 19*(7).

Valocchi, S. (2005). Not yet queer enough: The lessons of queer theory for the sociology of gender and sexuality. *Gender & Society, 19*(6), 750–770.

Veneklassen, L. & Miller, V. (2002). *A new weave of power, people and politics: The action guide for advocacy and citizen participation*. Practical Action.

Wagenknecht, A. (2014). Intro. In *Deep Lab* (9–12). Deep Lab.

Westin, A. (2015 [1967]). *Privacy and freedom*. Ig Publishing.

Whitson, J. (2015). Foucault's Fitbit: Governance and gamification. In S. Walz & S. Deterding (Eds.), *Gameful worlds: Approaches, issues, applications* (339–358). MIT Press.

Wood, D.M. (2017). Urban surveillance after the end of globalization. In J. Short (Ed.), *A research agenda for cities* (38–51). Edward Elgar.

Zaman, N. & Rudner, S. (2019). Reasonable expectation of privacy. *Canadian HR Reporter*. https://www.hrreporter.com/columnist/canadian-hr-law/archive/2019/02/19/reasonable-expectation-of-privacy/

Zuboff, S. (2019). *The age of surveillance capitalism*. Hachette.

Zuckerberg, M. (2019, May 1). *F8 day 1 keynote*. F8 Facebook Developer Conference, San Jose, CA.