Westminster Papers in Communication and Culture

Weinberg, L. (2017). Rethinking Privacy: A Feminist Approach to Privacy Rights after Snowden. *Westminster Papers in Communication and Culture,* 12(3), 5–20, DOI: https://doi.org/10.16997/wpcc.258

RESEARCH ARTICLE

Rethinking Privacy: A Feminist Approach to Privacy Rights after Snowden

Lindsay Weinberg
University of California, Santa Cruz, US
laweinbe@ucsc.edu

Tim Cook's message to Apple customers, regarding Apple's refusal to provide the FBI with a backdoor to the San Bernardino shooter's iPhone, typifies the corporate appropriation of privacy rights discourse. In light of this appropriation, I propose a reconsideration of the sovereign subject presupposed by privacy rights discourse through a comparative approach to the US and EU's treatments of privacy rights. I then apply feminist theories of the non-sovereign subject, which challenge liberal democratic discourse's construction of the subject by emphasising social interdependence. I argue that critical scholars of surveillance and the digital economy need to address the fact that the digital economy is predicated on the subject's non-sovereignty, where individuals can be fragmented and combined into the mass collection of data. I conclude with a discussion of how the non-sovereignty of the subject under commercial surveillance could also provide the grounds for the socialized redistribution of big data profits.

Keywords: feminism; privacy; surveillance; digital economy; user data

Introduction

On 2 December 2015, Syed Rizwan Farook and Tashfeen Malik killed fourteen people at the Inland Regional Center in San Bernardino, California. Magistrate Sheri Pym later issued a court order for Apple to provide the FBI with access to an iPhone belonging to one of the shooters. On 16 February 2016, Tim Cook, the CEO of Apple, released a message to customers on the company's website regarding this court order. Cook describes the FBI's demand as the following:

> Specifically, the FBI wants us to make a new version of the iPhone operating system, circumventing several important security features, and install it on an iPhone recovered during the investigation. In the wrong hands, this software — which does not exist today — would have the potential to unlock any iPhone in someone's physical possession. The FBI may use different words to describe this tool, but make no mistake: Building a version of iOS that bypasses security in this way would undeniably create a backdoor. And while the government may argue that its use would be limited to this case, there is no way to guarantee such control. (Cook, 2016)

Unbridled government access to personal cell phones certainly raises concerns over privacy, but what is particularly interesting about Cook's letter is the ways it posits Apple as a guarantor of such privacy. Apple is willing to confront the US government in the court of law in order to 'protect' the privacy of its users. And yet, the digital economy, which includes the goods and services that Apple provides, is predicated on the extraction and commodification of user data in order to market goods, services, and advertisements. Tech corporations are able to deploy the discourse of privacy rights to defend the aggregation of data against government abuses and yet simultaneously continue the collection of consumer data for the purposes of economic exploitation.

Another example of the corporate appropriation of privacy rights discourse – a discourse that was reignited by privacy rights activists following the Edward Snowden revelations – is the case of Uber, who on 2 January 2017 sent an email to registered users explaining that New York City policy makers were seeking to force Uber to disclose location data, particularly when users are dropped off. Uber writes that several 'independent privacy experts' have said that this policy would create serious privacy risks, resulting in a '*360-degree view into the movements and habits of individual New Yorkers*' (personal communication, emphasis in original). The intention of this email is to solicit the user to send an auto-generated email to the Taxi and Limousine Commission to express their discontent with the policy proposal. Uber markets itself as providing conditions of freedom, flexibility, and independence for its users and its workers, conditions that are threatened by this policy's potential to undermine consumer privacy. And yet, Uber's business model is contingent on the exploitation of their workforce through user data. Consumer data and the constant monitoring of user and worker behavior is instrumental to Uber's ability to set rates, performance targets, suggest schedules, and manage fluctuations in demand. Riders are able to provide feedback that directly affects the terms of employment for Uber drivers (Rosenblat, 2016). User data also helps Uber to forecast demand and thus keep their independently contracted workforce, or 'driver-partners' to use Uber's preferred terminology, temporary, flexible, and without the benefits that must be provided under conditions of full-time employment (Rosenblat, 2016). Both of these examples illustrate how corporate defenses of privacy rights serve as forms of instrumental corporate social responsibility in that these companies are framing themselves as defenders of user privacy, despite the fact that it is in their commercial interests to do so; on the one hand, these companies are cultivating affective bonds with their users over privacy concerns, and on the other, they are consolidating power and ownership over the data they collect.

In the context of this corporate appropriation of the struggle against surveillance through privacy rights discourse, the relationship between surveillance and privacy warrants rethinking. Rather than arguing that government and corporate surveillance encroaches on the private sphere, I argue that divisions between private and public are structured by the spatial organization of capital. The digital economy hybridizes public and private life through perpetual surveillance and its corresponding social practices. Privacy rights discourse, indebted to the liberal democratic tradition, reinforces the dichotomy between public and private life and also the fiction of the sovereign subject — a subject that 'answers only to its own [internal] order and is not accountable to a larger… community, save only to the extent is has consented to do so' (Bederman, 2001, 50). Feminist political philosophers, as I will later demonstrate, argue that liberal democratic discourse and its attending conceptual frameworks have failed to create conditions of equality for all subjects (Pateman, 1988; Kittay, 1999). In the liberal-democratic tradition's presupposition of individual subjects as free, self-possessive, and equally able of entering into contracts, the exploitation of contractual relations and the historical exclusion of women from the category of the individual remain concealed. Similarly, the notion of a separated, isolated private sphere conceals the ways the public sphere structures and impacts the regulation of private life, often to the detriment of women.

Following feminist political theory's critique of the public-private divide and the fiction of the sovereign subject, I argue that the focus in a critical analysis of the digital economy should not be on the ways commercial surveillance has come to encroach upon an otherwise isolated private sphere, but rather on the points in the circulation of capital where subjects are individuated or dividuated for the purposes of extracting profit. I define individuation as the construction of the consuming, desiring, producing, individual subject, and dividuation, following Gilles Deleuze (1992), as the processes whereby subjects are treated as an aggregated and anonymised mass, and are thus non-sovereign. Whereas for Karl Marx (1992), the primary tension was between subjectivity (workers as commodity owners) and objectivity (workers as objects of the capitalist process of production/as commodities themselves), the tension produced in a social order mediated not only by the commodity, but also by the information asset, is a tension between individuation and dividuation.

Methods

Immanent critique, which emphasises the underlying assumptions and contradictions within privacy rights discourse, allows me to demonstrate that privacy rights and proprietary ownership are imbricated in privacy rights discourse, a discourse functioning to the benefit of capitalists, who are able to claim as their private property the data of others. I examine how the subject is constituted in legal policy concerning privacy and the production of data through a comparative approach to the US and the EU's treatments of privacy rights issues. In the EU, privacy is treated as a human right – particularly a right to dignity, where the state is seen as a guarantor of such a right. In the US, privacy is conceptualised as liberty from unreasonable government surveillance. Contracts in the US context, between employers and employees, or platform providers and users, are widely accepted as setting the terms for the right to privacy. I analyse debates over privacy and data legislation as examples of the advantages and limitations of privacy rights discourse, and then describe the implications of the recently overturned 'Safe Harbor' agreement in the United States.

The final task of this article will be to put Deleuze's concept of dividuation in conversation with feminist theories of the non-sovereign subject. The accumulation of large bodies of data from an aggregate of subjects – dividuation – is what allows surveillance to produce predictive and logistical analytics. The concept of individual privacy rights reinforces the idea of the juridical, rights-bearing subject of liberal democracy rather than the dividuated, disembodied, deterritorialised subject of communications networks. Deleuze's concept of dividuation reveals the following: that political economy is predicated on the construction of the liberal sovereign subject for the sake of organising the relationship between the state and civil society, *and* an ability to fragment the individual subject into data that can then be aggregated for the purposes of managing populations and goods. Theories of the non-sovereign subject, including Eva Feder Kittay's *Love's Labor* and Carole Pateman's *The Sexual Contract,* provide a feminist moral and political philosophy that challenges the construction of the sovereign subject in liberal democratic discourse. I use this feminist approach to political philosophy to think through what a politics of the dividual might look like, meaning how the non-sovereignty of the subject under commercial forms of surveillance could also potentially provide the groundwork for a transformative politics by stressing the productive power of relational subjects in the digital economy, who could stake claims on big data profits.

Public and private in the digital economy

Conceptual divisions between labour and leisure and public and private are the foundation of liberal democratic theories of the subject. On the first distinction, subjects have the freedom to sell their labour power in the market place, to have that labour exchanged for

a wage, and to have that wage provide a means of enjoying leisure. Similarly, the subject is presupposed to have rights and obligations in a clearly parsed out separation between public and private life, where public life encompasses the subject's time outside the home in which government and workplace surveillance is legally codified, and private life is a space protected from the encroaching power of the state. Workplace discipline and surveillance are readily accepted because of their association with time that is not free but owned by the capitalist. It is assumed that one's leisure time in the private domestic space is owned by oneself, and therefore should not be subject to monitoring.

While the private sphere has been presented as separate and opposed to the public sphere, feminist theorists have demonstrated their interrelatedness. The slogan 'the personal is political' is often cited as an example of the challenge to the division between public and private life, given the ways the private sphere is structured by decisions made in the public sphere, often to the detriment of women (Hanisch, 1970). Whereas traditional liberal democratic theory posits the separation and opposition of public and private life, feminists worked to develop a general theory of social practice grounded in the idea that individual and collective life are interrelated (Pateman, 1989, 135). For Pateman, challenging the dichotomy between public and private was instrumental to the women's movement. And yet, the digital economy – in its hybridization of public and private life where the private is increasingly publicized, commodified, and subject to state and corporate surveillance – establishes the private as public without the underlying politics of women's liberation. Users are able to 'blur the boundaries of work and home, school and private life, or friends and family' and engage in acts of self-disclosure and social surveillance of both public and private life (Marwick, 2012, 379). As Diana Coole (2000) explains in the context of a global communications network that merges public and private life, spaces are increasingly mobile and connected, and thus destabilise a clear boundary between the public and private. Coole argues that 'while the response of some critics, feminists among them, has been to reach for a liberal language of negative liberty, privacy, and protective rights, these would seem to have only marginal relevance to the sort of processes mentioned here' (p. 349). For Coole, an adequate theory of the public and private needs to account for the transformations in space and power brought about under postmodernism (p. 353). Privacy rights, which are certainly effective in tempering certain forms of discrimination and government oversight in that they provide a legal framework for contestation, maintain a dichotomy between public and private life; a dichotomy inadequate for understanding the political economy and cultural practices of the digital economy. An understanding of the public-private distinction in the digital economy needs to adequately address the ways that conceptions of the private and public have been transformed by technology, including commercial surveillance.

While recent surveys convey that Internet users have concern about personal privacy online (Madden & Rainie, 2015), digital culture often relies upon the publicity of private life. Ursula Frohne (2002) posits that in light of social media and the relationship between self-presentation, self-promotion, and online surveillance, 'What is to be feared, then, is perhaps less the threats to our privacy from a panoptic media culture… than the social and cultural devaluation of anonymity, the erosion of introspective and un-televised moments of life' (p. 256). There is a tension between user desire for protection from the invasive oversight of governments and corporations online and the willing disclosure of personal information, pictures, location data, preferences, habits, and desires. Capital's intensified exploitation of the private realm goes hand in hand with the cultural association of submission to technologies of surveillance with self-expression and empowerment for many online users. These cultural practices destabilize the clear division between public and private life that liberal democratic theorists like John Stuart Mill (1864), Jürgen Habermas (1991), and Hannah Arendt (1958)

argued were essential to democracy. Under digital culture, surveillance extends throughout social life.

The digital economy thus fosters not only a hybridization of the public and private spheres, but it also merges capitalist and public interests, given the direct economic exploitation of both spheres. As Zizi Papacharissi (2010a) explains, 'information about decision-making behaviors that occur in the private realm increasingly becomes a tradable commodity' (p. 45). This information, assembled by private data brokers, is marketed and sold to both private and state entities. For example, the Digital Recognition Network collects surveillance data on most vehicles registered in the United States. Repossession and insurance companies, as well as the police, use this data (Musgrave, 2014). The subject's active engagement with digital culture thus simultaneously produces her as an object of market and state knowledge. What current privacy rights frameworks struggle to account for, given the emphasis on individual rights-based claims, is the process of dividuation – the *mass* data aggregation that allows for the prediction and governance of subjects' behavior and choices – on which the digital economy is predicated.

Comparative analysis of privacy rights discourse in the EU and the US

Privacy rights discourse first emerged in the United States in the late nineteenth century. While the US Constitution limited federal power over 'unreasonable search and seizure' in 1787 through the Fourth Amendment, the idea of the 'right to privacy' first emerged in 1890 (Solove, 2006). New visual technologies and the emergence of mass media were framed as a threat to the self-possessive individual's right to autonomy and freedom from personal injury. Specifically, as Eden Osucha (2009) explains, popular anxieties about the exposure and commodification of white womens' bodies raised by the popularization of photography culminated in the right to privacy, working to 'stabilize a conventionally gendered division between public and private by replacing this outmoded and increasingly unsupportable distinction with a set of cognate terms – namely, *publicity* and *privacy* – uniquely adapted to the mass-mediated public sphere (p. 72). Samuel Warren and Louis Brandeis (1890) famously argued that only a more expansive understanding of property rights could ensure someone's private portrait wasn't misused. Thus, from its inception in the US, privacy rights were framed as a right to the property of oneself, a right of self-interest and individual liberty.

One of the first legislative acts in the US explicitly related to privacy was in response to public anxieties over Watergate, which had revealed the government's abuse of surveillance. In 1974, the Privacy Act was passed that mandated that the government keep records only if necessary and released only with the individual's consent, excluding the security needs of government and law enforcement (United States Department of Justice, 2015a). The Electronic Communications Privacy Act of 1986 imposed similar limitations on unauthorized government surveillance (United States Department of Justice, 2015b). While this legislation addresses subjects' concerns over direct government surveillance, government agencies, including the Departments of Justice, Homeland Security, and State and the Social Security Administration, continue to engage in practices of buying data collected by private interests (Schneier, 2013). Unlike the EU, which I will discuss below, the primary means of addressing privacy concerns is through real or threatened litigation over common law tort claims. There are certain statutes meant to limit the exchange of data between private interests and help subjects ensure the accuracy of the data about them, such as the Fair Credit Report Act (Federal Trade Commission, 2016a) and the Financial Services Modernization Act of 1999 (Federal Trade Commission, 2016b), which also mandates that consumers should have the choice of opting out of sharing their credit information. However, these laws only apply to personally identifiable information, not data in the aggregate.

In many cases, privacy legislation has been used to expand the scope of capitalist surveillance rather than impose limits. For instance, the Video Privacy Protection Act (VPPA) of 1988 was initially passed to prevent the disclosure of an individual's personal rental viewing habits after a Supreme Court nominee's records were published in a newspaper. The VPPA stipulated these records should remain private unless the consumer grants expressed permission or the records are subpoenaed. This act became the foundation for Netflix's 2011 push to amend the VPPA's consent provision so that companies could obtain a one-time consent from consumers, allowing Netflix, and other platforms like Facebook, to use the association of users with various commodities and services to create targeted ad campaigns (Electronic Privacy Information Center, 2016). While Facebook did lose a $20 million lawsuit over their Sponsored Stories target advertising campaign, which used the actual images of its users and their corresponding likes to advertise to the user's network, this was because Facebook had yet to update their terms of service (TOS). Currently, the TOS have been updated, and there is no way to opt-out other than to quit Facebook (Roberts, 2013). While Colin J. Bennett (2011) contends that, 'Realistically, without privacy regimes, there would be few if any actual mechanisms of social redress for public and private wrongs. And sometimes, the policy regimes do have positive results,' (p. 494) privacy regimes centered on rights and contractual relations between individuals and corporations also help corporations to modify TOS in order to further legitimate data expropriation as mutually agreed upon and transparent.

As these examples demonstrate, contracts set the terms of privacy between users and platforms. The option to opt-out results in users losing access to the necessary services for finding jobs, connecting with friends, and impedes the successful functioning of many sites. Frank Pasquale (2013) explains that privacy regimes based on notice-and-consent also 'privilege on-the-fly consumer judgments to "opt-in" to one-sided contracts over a reflexive consideration of how data flows might be optimized for consumers' interests in the long run' (p. 1011). According to Felix Stalder (2010), a conception of privacy founded on individualism does not hold up against a networked society, which requires electronic connections and constant data sharing. Post-Fordist societies of control, meaning societies structured by the continuous flow of information across social and institutional arrangements (Deleuze, 1992), require entering into relationships that constantly produce electronic, personal data that is aggregated and exchanged between services and institutions. Privacy rights enacted through contracts legally protect the interests of corporations who can claim they uphold privacy rights through the documented record of user consent. Regulatory policy in the US operates on the assumption that 'web operators should disclose, but not adjust or restrict, information gathering and use practices' (Papacharissi, 2010a, 45). The impetus is on users to perform autonomous self-management and cultivate the skills and literacy necessary for determining whether to engage with certain services and platforms. Additionally, while some platforms provide opt-outs for target ads, rarely can a user opt out of having their information tracked (Hill, 2012).

In the EU, privacy rights similarly emerged in the nineteenth century in response to the technological possibilities of photography. Alexandre Dumas, author of *The Three Musketeers,* and his lover, Adah Isaacs Menken, were photographed in a scandalous embrace. These photographs were later sold, and Dumas was able to successfully have the photographs taken out of circulation by order of a Paris appeals court (Sullivan, 2006). From its inception, privacy was framed in the EU as an explicit right to dignity and self-determination. This necessarily ties the data of concern to EU law as data that is personally identifiable, as is the case in the United States. In the European Union Data Directive of 1995, personal data is defined as 'any information related to an identified or identifiable natural person...who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his psychical, physiological, mental, economic, cultural or social identity'

(European Union, 1995). The directive explicitly states, 'the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable' (European Union, 1995). Multinational opponents, lobbying the EU, maintain the same defense; that anonymized data are not personal data (Szekely, 2014, 34). Privacy advocates often criticize the directive as being out of touch with the Internet era, an era in which the sharing of personal information is practically a prerequisite for engaging in social media (Szekely, 2014, 72). This criticism helped inspire the European Commission's 'Proposal for a Regulation on the Protection of Individuals with Regard to Processing of Personal Data and on the Free Movement of Such Data' adopted in 2012, which included the Right to be Forgotten, a right in which a person can have data that was given either voluntarily or involuntarily removed from Internet search engines if the data is deemed irrelevant, no longer relevant, or inadequate (European Commission, 2012). This right reflects the EU's investment in minimizing the potential of personal data to stigmatize and damage an individual's reputation, job prospects, and well-being, but it is also up to the data controller to determine whether it is in the public interest for the information to remain accessible online, and whether the data meets the criteria outlined in the proposal (Arthur, 2014).

While the EU and the US conceptualize privacy differently, privacy is framed in both cases as a right belonging to a particularized subject. The idea of the sovereign subject certainly helps to impose limits on big data; the rights-bearing subject can use channels offered within a liberal-democratic political framework to contest unlawful uses of data for discrimination and political persecution. The sovereign subject, regardless of whether it is a construction dependent on the recognition of state power, provides a way to resist some corporate and government abuses of technologies of surveillance and data aggregation. In the EU in particular, the notion of personal dignity and the right to be forgotten reflect the ways that subjects understand data aggregation as having drastic consequences for the ability to enjoy job security, be protected against libellous speech, and not be forever tied to past actions that are then outside the individual's control. These measures have been less popular in the US context, which discursively prioritizes free speech and the constitutional protections it affords.

These tensions and differences between the US and EU recently resulted in the overturning of the Safe Harbor Agreement in 2015. The agreement had given US corporations the ability to transfer huge quantities of data containing EU citizens' personal information to the United States. The Snowden revelations prompted Max Schrems to file a complaint with the Irish data protection commissioner that ultimately ended up in the Court of Justice of the European Union (CJEU). The CJEU determined that Facebook violated the EU Data Protection Directive by making EU citizen data accessible to US intelligence collection (Lomas, 2015). The overturning of the Safe Harbor Agreement is certainly a victory for privacy rights activists and will hopefully succeed in imposing greater oversight and restrictions on the transfer of personal data, but it only emphasizes concern over government misappropriation of data, when it should also deal with the conditions of exploitation that underlie capitalist surveillance for data aggregation.

While advocates of privacy use the fiction of the sovereign subject to resist surveillance, corporations and governments have found ways to continue aggregating data in ways that are technically lawful. In anonymizing data, these institutions can argue they uphold the legal protections afforded to users in regard to individual privacy and concerns over discrimination. According to Mark Andrejevic (2002):

> The attempt to defend privacy rights has a disconcerting tendency to work as much in the interest of corporations doing the monitoring as in that of the individuals being monitored. The development of demographic databases relies heavily on the

> protection accorded to private property, since these databases are profitable in large part because the information they contain is proprietary.' (p. 232)

Services like Datacoup have been created to help users 'take control' of their data, to bring their data to market just like their capacity for labour in the workplace (Datacoup, 2013). Datacoup relies on the user to assemble the data on the platform's behalf by linking his/her demographic data, search behavior, and credit card, among other details, and by then setting a price for which companies and data brokers might purchase the data. While the marketing of these services often calls attention to the fact that free services online depend on the extraction of data, the ability to exchange one's private information for a wage merely reproduces the power asymmetries of the workplace. Target advertising, for instance, provides users that are most likely to provide a return on capitalist investment with particular options and choices, while those determined to be risky investments do not receive the same rates, discounts, and ads (Davidow, 2014). The reward of cost-saving and fast shipping for Amazon customers is contingent upon the hyper-Taylorization of the fulfillment centre made possible by aggregate consumer and worker data (McClelland, 2015). Much like traditional labour produces surplus value that is not returned to the worker, consumer data produces valuable surplus information that is used to exploit consumers and workers alike.

For most people, access to services that have become instrumental to securing a job, spending efficiently, and/or maintaining social bonds takes precedence over privacy. As Papacharissi (2010b) explains, privacy begins to function as a luxury commodity when it is only enjoyed by those who can afford to forsake the goods and services that otherwise require the relinquishing of privacy or who can afford to pay subscription fees to avoid being targeted. For those who are in a position to sacrifice access to these services, enacting privacy generally requires 'a level of computer literacy that is inaccessible to most, and typically associated with higher income and education levels, and certain ethnic groups, in ways that mirror dominant socio-demographic inequalities' (Papacharissi, 2010b). This creates what Papacharissi describes as a privacy divide between those who have the means to opt-out and those who do not.

The ability to exchange one's data for a wage helps socialize users to willingly relinquish privacy, while providing no recourse for users regarding how the information is instrumentalised. Additionally, and as argued above, the notion of privacy does not include the practices of surveillance where data is aggregated and anonymized, thus curtailing many legal efforts to hold companies accountable for discriminatory practices. While the effort to protect the privacy of individuals certainly helps to mark certain government and business practices as discriminatory, profit is mostly extracted from anonymized data in the aggregate, and therefore upholds the legal standards of privacy rights. Perhaps then, the reliance on the sovereignty of the individual subject under the liberal-democratic tradition prevents a more transformative politics from coming to the fore.

Dividuation and theories of the non-sovereign subject

Selfhood and inalienable rights are predicated on the indivisibility of the subject, and yet, the digital economy relies on the divisibility of the subject under control societies, a subject who is 'endlessly divisible and reducible to data representations via the modern technologies of control, like computer-based systems' (Williams, 2005). Deleuze's concept of dividuation fundamentally undermines the conception of the individual presupposed by Western philosophy and political theory. The idea of the unitary self is central to traditional economic theory, political science, and legal analysis (Williams, 2005). If, as I have argued, discourses about privacy rights are tethered to the idea of the sovereign self, and if this tethering has

provided loopholes that can be exploited by corporate interests, what theory of the subject might be able to encompass this Deleuzian framework for rethinking privacy?

Feminist theory has been one of the most generative sites for theories of the non-sovereign, relational subject. Carole Pateman (1988) has criticized the sovereign subject of liberal democratic discourse for concealing patriarchal social relations and for presupposing the male, and I would add following Charles W. Mills (1999), white, body. Pateman explains that the employment contract and the marriage contract render workers and wives exploited. Contracts are premised on 'exemplifying and securing individual freedom. On the contrary, in contract theory universal freedom is always an hypothesis, a story, a political fiction. Contract always generates political right in the form of relations of domination and subordination' (Pateman, 1988, 8). The contestation over privacy rights not only perpetuates a dichotomy between the private and public sphere that appears outmoded given the cultural and economic hybridization of these spaces, but also conceals the social relations between online users that produce the unequal distribution of risks and rewards for social actors (Davidow, 2014). Privacy rights, in their emphasis on the individual's proprietary ownership over privacy, foster the sense that freedom is achievable through contract and ownership. In the same way that workers must agree through contract to be subordinate to their employer, privacy rights put the subject in the position of either agreeing to be exploited, or to not participate in digital culture. While the non-political status of familial and private life conceals the contractual relationship of marriage that produces the family (Pateman, 1988, 94), the privacy rights framework conceals the non-sovereignty of online users who are governed through the commercialized capacity to distill patterns in aggregate data.

For Pateman, contract theory does not provide feminists with an adequate politics of resistance against patriarchy. She explains, 'it is tempting for feminists to conclude that the idea of the individual as owner is anti-patriarchal. If women could be acknowledged as sexually neutered 'individuals', owners of the property in their persons, the emancipatory promise of contract would seem to be realized' (Pateman, 1988, 153). Pateman argues that the desexing of the body on which contract theory is premised cannot be restored through the appropriation of the category of the 'individual,' which always already conceals the sexual division of labour on which capitalist, patriarchal society is founded upon (Pateman, 1988, 153). This concealment in the context of privacy online is also a concealment of class relations, given that those able to exercise their right to privacy are in a position to opt-out or afford the legal contestation over corporate or government surveillance.

Eva Feder Kittay (1999) is another feminist theorist who is critical of the liberal democratic theory of the sovereign subject. For Kittay, 'a conception of society viewed as an association of equals masks inequitable dependencies, those of infancy and childhood, old age, illness and disability. While we are dependent, we are not well positioned to enter a competition for the goods of social cooperation on equal terms' (Kittay, 1999, xi). Kittay is primarily concerned with the lack of recognition and support for relations between caretakers and dependents that are otherwise masked by the understanding of society as an association of equals, but her emphasis on the interdependence of subjects helps inform a theory of non-sovereign subjects in the digital economy. Kittay proposes that rather than focusing on the properties that make people individuals – rationality, self-interest – we could formulate an equality based on mutual relations of care and concern (p. 28). Kittay's framework recognises inequalities in power, and relations of dependency, rather than any presumed equality. A transformative politics for Kittay is premised on the inevitability of human interdependence. Rather than essentializing these conditions of dependence as transhistorical, I propose that Kittay's framework of subject interdependence can also be used to characterize the relationality of subjects in the digital economy. The economization and individualization of social life online

conceals the process of dividuation on which the digital economy is premised. Moreover, the privileging in privacy rights discourse of the private sphere that needs to be restored risks perpetuating a dichotomy between public and private life that no longer adequately describes the structural or cultural conditions of digital subjects.

Under post-Fordist societies of control, it is the ability to consolidate the actions of subjects through the fragmentation of subjective behavior into aggregate data that makes control possible. But while in Deleuze's framework, the dividual is disembodied and reduced to information flows within the circulation of capital, the dividual is also symptomatic of the underlying sociality underpinning post-Fordism, where the dependency and vulnerability of some subjects is coproduced alongside the incentives and rewards of other subjects. The contractual nature of consumers and platforms, where consumers 'freely' agree to the terms of service of platform providers, and the contractual nature of the labour contract, where workers 'freely' agree to exchange their labour power for a wage, conceals these social relations of power.

While industry insiders emphasize the importance of individual, personalized, web experiences, generating a conception of the self as unitary, non-relational, and rationally predictable through the perpetual celebration of the individual consumer's needs and the ability of the digital economy to respond to that individual consumer reflexively (Davenport & Beck, 2002), the underpinning process of dividuation reveals a relational and fragmented subject. As Tiziana Terranova explains, by the early 1990s, there was a push within marketing to develop advertising:

> Not simply directed at groups but tailored to individuals and even sub-individual units (or as Gilles Deleuze called them, 'dividuals', what results from the decomposition of individuals into data clouds subject to automated integration and disintegration). These patterns identified by marketing models correspond to a process whereby the postmodern segmentation of the mass audience is pursued to the point where it becomes a mobile, multiple and discontinuous microsegmentation. (Terranova, 2004, 34)

The microsegmentation of the market is predicated on the ability to aggregate data in order to create prediction and statistical analyses for the purposes of allocating risk and reward. It is not surprising then that subjects perform acts of centering, self-narrating, and confession online in order to restore a sense of unity to the post-Fordist fragmentation of the self. These practices are highly compatible with the imperatives of the digital economy that seek to commodify the subject's engagement with online platforms. Subjects are incentivized to relinquish personal data, preferences, desires, and habits as they engage with digital culture. The environment that the subject finds herself in, the kinds of prompts, incentives, and blockages she encounters, is conditioned by her relationship to the aggregated data of others. As Bent Meier Sorensen explains, 'your self is to be abstracted from databanks, registers, tests and focus group interviews, and the data is to be personalised in the "security" of passwords that you memorise. You will be asked to carry out this abstraction yourself' (Sorensen, 2009, 65). A transformative politics that might be less recuperable to the surveillance regime of the digital economy, then, would be a politics that does not seek to restore unity to the individual, but bases itself on a materialist analysis of the digital economy and its production of dividuals. The fragmentation and relationality of the subject underpinning dividuation can then become the grounds for making claims on the profits of big data in ways that are social rather than individual.

In Marx's (1973) *1857 Introduction,* he explains his skepticism of the individual as the unit of civil society. He argues that as the individual appears increasingly isolated in civil

society and engages in acts of private enterprise and exchange, the actual power relations underpinning society are socially intensified (p. 84). Later, Marx would extend this critique to the individual as citizen, who self-possesses a series of rights, arguing, 'political liberators reduce citizenship, the political community, to a mere means for preserving these so-called rights of man; and consequently, that the citizen is declared to be the servant of egoistic "man"' (Marx, 2003, 109). The social conditions that produce the unequal terms of exchange are otherwise concealed and naturalized by the system of exchange between seemingly independent and equal individuals (Marx, 1973, 164). According to Marx, individuals must be understood as socially produced through the forces of production and social relations, as social individuals (Marx, 1973, 706). What the forces of production and social relations underpinning dividuation reveal about the digital economy is that profit is accumulated using the collective aggregate of individual data, and it is this aggregate – not individual data – that helps produce the surplus. As Jason Read (2015) explains, 'the production of data through the use of social networking and search engines, as well as consumer data through shopping, functions less as an individual product, or even a collective endeavor, than the production of information that only functions across fragments and parts of identities' (p. 240). It is this aggregate data that informs the ways subjects are governed through their ability to make choices. The use of aggregate information about subjects in order to determine the options, incentives, and risks assigned to them is 'ideal for the masking of inequality, for the multiplication of opaque quantitative forms that are illegible to the average citizen, and for the multiplication of profit-making tools and techniques, which can escape audit, regulation, and social control' (Appadurai, 2015, 102).

If one were to understand dividuation not merely as the product of fragmentation and disembodiment wrought by digital economies, but as symptomatic of the sociality underpinning those digital economies, then one must refuse 'the false binary of the individual and society, examining the points of intersection of individuation and collective existence' (Read, 2015, 286). In the context of the digital economy, the very conditions that produce the subject as an individual, desiring, producing, consuming subject are based on the collective conditions of an aggregated and anonymized dividual through the extraction of information. It is the awareness of these collective conditions of dividuation that then empowers subjects to act collectively against conditions of exploitation and surveillance in the digital economy.

In response to the fundamental non-sovereignty and vulnerability of subjects emphasized by the possibility of violence and grief, Judith Butler (2004) explains relationality 'not only as a descriptive or historical fact of our formation, but also as an ongoing normative dimension of our social and political lives, one in which we are compelled to take stock of our interdependence' (p. 27). Current privacy rights frameworks do not facilitate collective contestation, but instead, treat privacy as a matter of individual rights, or what Marx might call 'the right of the *circumscribed* individual, withdrawn into himself,' founded not on relations between subjects but on their mutual separation (Marx, 2003, 108). The dividual thus presents a case for 'radically new forms of collective agency and connectivity that can replace the current predatory forms of dividualism with truly socialized dividualism' (Appadurai, 2015, 102) rather than a return to the classical, masculinist tradition of individualism within liberal democratic discourse. A political framework that centers on dividuation accounts for interdependence, and how this interdependence is embedded within the surveillance regime of the digital economy to produce inequality rather than collective ownership over the means of communication and information collection. A socialized dividualism would reject the unequal distribution of risks and rewards and the precarious, hyper flexibility of the labour market and call for the redistribution of wealth produced out of aggregate data.

Conclusion

Without critically engaging the underlying assumptions of the categories of public and private, the forms of political resistance against data exploitation remain tethered to presuppositions about the liberal democratic subject. Concerns over individual privacy rights tend to obfuscate how information technologies produce profit; profit is produced through the aggregate of anonymized data from all users that then allows for predictive analytics to determine who is most likely to provide a return on capitalist investment. As far as the creation of profit is concerned, what takes precedence is not the individual behavior of particularized and identifiable users, but the ability to formulate patterns and determine risk and opportunity for investment in order to effectively allocate advertisements, goods and services. By anonymizing data, corporations are able to uphold the protections afforded to individuals, despite the fact that the stratification of risk and opportunity further entrench inequality.

What, then, might a transformative politics look like concerning the digital economy if the traditional categories of the public and private are no longer tenable distinctions, or put in the service of the extraction of profit for the few? The recognition of the non-sovereignty of the subject under commercial forms of surveillance could also potentially provide the groundwork for a transformative politics in that it stresses relationality between subjects; the contingencies between subjects in that one person's data extracted through leisure-time surveillance could be used to intensify the work-place domination of another, or that profit is produced not through the infringement upon individual rights to privacy but through the aggregate of subjects in ways that allow for prediction, preemption, and the management of options and choices for individuals. Thus, conceptual distinctions between public and private provide some opportunities for resistance, but these demands ultimately treat collective conditions of dividuation as a matter of individual rights to privacy.

This article has demonstrated the limitations of privacy rights discourse for scholars seeking to formulate a critique of the digital economy. Subject formations and divisions between public and private are destabilized when the totality of social time becomes part of social production, when the mode of production is based on capturing not only surplus value but also surplus information. Rather than data being put to use for the unequal distribution of social risks and rewards and for economic exploitation, perhaps data could be harnessed in ways that benefit all. A privacy rights framework risks reducing the totality of the digital economy and its attending conditions of exploitation to a matter of individual rights rather than a social condition. At minimum, the current private economization of data that results in the unequal distribution of market choices, flexible and precarious labour, and the consolidation of power, information, and wealth in the hands of the few should be socialized; the repurposing of surplus wealth extracted from corporations that exploit user data for social uses. Socializing big data profits could take many forms: a basic income, or funding for free public health care and education, for example. Forms of wealth redistribution and the contestation of big data power relations are already taking place in the platform cooperativist movement, which envision collective ownership, transparency around data harvesting, limits on workplace surveillance, and democratic governance (Scholz, 2016). The Robin Hood Asset Management Cooperative, for instance, is a co-op hedge fund that mines the movements of Wall Street's investors using an algorithm called the 'parasite' and redistributes these profits into 'projects building the commons' (Robin Hood Cooperative, 2017). These demands and experimental tactics for the redistribution of corporate wealth simultaneously work to make the conditions of collective surveillance and data aggregation visible, and ultimately, contestable.

Acknowledgements

This article was made possible through funding from the Institute for Humanities Research, crucial feedback from Stephen David Engel, as well as the guidance of Professors Robert Meister, Carla Freccero, Warren Sack, and Mark Andrejevic. The author would also like to thank the peer reviewers and editors of *Westminster Papers in Communication and Culture* for their insightful comments.

Competing Interests

The author has no competing interests to declare.

References

Andrejevic, M. (2002). The work of being watched: Interactive media and the exploitation of self-disclosure. *Critical Studies in Media Communication*, 19(2): 230–248. DOI: https://doi.org/10.1080/07393180216561

Appadurai, A. (2015). *Banking on Words: The Failure of Language in the Age of Derivative Finance*. Chicago, IL: University of Chicago Press. DOI: https://doi.org/10.7208/chicago/9780226318806.001.0001

Arendt, H. (1958). *The Human Condition*. Chicago, IL: University of Chicago Press.

Arthur, C. (2014). Explaining the 'right to be forgotten' – the newest cultural shibboleth. *The Guardian*, 14 May. Retrieved from: https://www.theguardian.com/technology/2014/may/14/explainer-right-to-be-forgotten-the-newest-cultural-shibboleth.

Bederman, D. J. (2001). *International Law Frameworks*. Eagan, MN: Foundation Press.

Bennett, C. J. (2011). In defense of privacy: The concept and the regime. *Surveillance and Society*, 8(4): 485–496. Retrieved from: http://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/4184.

Butler, J. (2004). *Precarious Life*. London: Verso.

Cook, T. (2016). A message to our customers. 16 February. Retrieved from: http://www.apple.com/customer-letter/.

Coole, D. (2000). Cartographic convulsions: Public and private reconsidered. *Political Theory*, 28: 337–354. DOI: https://doi.org/10.1177/0090591700028003002

Datacoup. (2013). About Us. Retrieved from: https://datacoup.com/docs#how-it-works.

Davenport, T. H., & **Beck, J. C.** (2002). *Attention Economy: Understanding the New Currency of Big Business*. Cambridge, MA: Harvard Business Review Press.

Davidow, B. (2014). Redlining for the 21st century. *The Atlantic*, 5 March. Retrieved from: http://www.theatlantic.com/business/archive/2014/03/redlining-for-the-21st-century/284235/.

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

Electronic Privacy Information Center. (2016). Video privacy protection act. Retrieved from: https://epic.org/privacy/vppa/.

European Commission. (2012). Proposal for a regulation on the protection of individuals with regard to processing of personal data and on the free movement of such data. *Eur-Lex*. Retrieved from: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A52012PC0011.

European Union. (1995). Directive 95/46/EC of the European Parliament and the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Oct. 24. Retrieved from: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

Federal Trade Commission. (2016a). Fair credit reporting act. Retrieved from: https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/fair-credit-reporting-act and Federal Reserve Bank of Minneapolis.

Federal Trade Commission. (2016b). The financial services modernization act of 1999. Retrieved from: https://www.minneapolisfed.org/publications/the-region/the-financial-services-modernization-act-of-1999.

Frohne, U. (2002). 'Screen tests': Media narcissism, theatricality, and the internalized observer. In: Levin, T. Y., Frohne, U., & Weibel, P. (eds.), *CTRL Space: Rhetorics of Surveillance from Bentham to Big Brother*, 252–278. Cambridge, MA: MIT Press.

Habermas, J. (1991). *The Structural Transformation of the Public Sphere: An Inquiry into Bourgeois Society*. Cambridge, MA: MIT Press.

Hanisch, C. (1970). The personal is political. In: Firestone, S., & Koedt, A. (eds.), *Notes From the Second Year: Women's Liberation: Major Writings of the Radical Feminists*, 76–78. New York: Radical Feminism.

Hill, K. (2012). Don't want to be targeted by target? There's an opt out. *Forbes*, 22 February. Retrieved from: http://www.forbes.com/sites/kashmirhill/2012/02/22/dont-want-to-be-targeted-by-target-theres-an-opt-out/#3a10ac9c7d4c.

Kittay, E. F. (1999). *Love's Labor: Essays on Women, Equality, and Dependency*. New York: Routledge.

Lomas, N. (2015). Europe's top court strikes down 'safe harbor' data-transfer agreement with us. *Techcrunch*, Oct. 6. Retrieved from: https://techcrunch.com/2015/10/06/europes-top-court-strikes-down-safe-harbor-data-transfer-agreement-with-u-s/.

Madden, M., & **Rainie, L.** (2015). Americans' attitudes about privacy, security and surveillance. *Pew Research Center: Internet and Technology*, 20 May. Retrieved from: http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/.

Marwick, A. E. (2012). The public domain: Social surveillance in everyday life. *Surveillance and Society*, 9(4): 378–393. Retrieved from: http://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/pub_dom/pub_dom.

Marx, K. (1973). *Grundrisse: Foundations of the Critique of Political Economy*. London: Penguin Books.

Marx, K. (1992). *Capital: Volume 1: A Critique of Political Economy*. London: Penguin Random House.

Marx, K. (2003). On the Jewish question. In Hodgkinson, V., & Foley, M. (eds.), *The Civil Society Reader*, 96–112. Lebanon, NH: University Press of New England.

McClelland, M. (2015). I was a warehouse wage slave. *Mother Jones*, 3 February. Retrieved from: http://www.motherjones.com/politics/2012/02/mac-mcclelland-free-online-shipping-warehouses-labour.

Mill, J. S. (1864). *On Liberty*. London: John W. Parker and Son.

Mills, C. W. (1999). *The Racial Contract*. Ithaca, NY: Cornell University Press.

Musgrave, S. (2014). These are the slides digital recognition network uses to sell police and repo companies on its license plate surveillance database. *Boston Globe*. Retrieved from: http://www.betaboston.com/news/2014/03/11/these-are-the-slides-digital-recognition-network-uses-to-sell-police-and-repo-companies-on-its-license-plate-surveillance-database/.

Osucha, E. (2009). The whiteness of privacy: Race, media, law. *Camera Obscura*, 24(1): 67–107. DOI: https://doi.org/10.1215/02705346-2008-015

Papacharissi, Z. (2010a). *A Private Sphere: Democracy in a Digital Age*. Cambridge: Polity.

Papacharissi, Z. (2010b). Privacy as a luxury commodity. *First Monday*, 15(8). Retrieved from: http://firstmonday.org/ojs/index.php/fm/article/view/3075/2581. DOI: https://doi.org/10.5210/fm.v15i8.3075

Pasquale, F. A., III. (2013). Privacy, antitrust, and power. *George Mason Law Review*, 20(4): 1009–1024.

Pateman, C. (1988). *The Sexual Contract*. Stanford, CA: Stanford University Press.

Pateman, C. (1989). *The Disorder of Women: Democracy, Feminism and Political Theory*. Stanford, CA: Stanford University Press.

Read, J. (2015). *The Politics of Transindividuality*. Leiden, Netherlands: Brill. DOI: https://doi.org/10.1163/9789004305151

Roberts, J. (2013). Here's why it's legal for Google and Facebook to use your face in ads. *Gigaom*, Oct. 15. Retrieved from: https://gigaom.com/2013/10/15/heres-why-its-legal-for-google-and-facebook-to-use-your-face-in-ads/.

Robin Hood Collective. (2017). What is Robin Hood? Retrieved from: http://www.robinhoodcoop.org/.

Rosenblat, A. (2016). The truth about how Uber's app manages drivers. *Harvard Business Review*, Apr. 6. Retrieved from: https://hbr.org/2016/04/the-truth-about-how-ubers-app-manages-drivers.

Schneier, B. (2013). Do you want the government buying your data from corporations? *The Atlantic*, 30 April. Retrieved from: http://www.theatlantic.com/technology/archive/2013/04/do-you-want-the-government-buying-your-data-from-corporations/275431/.

Scholz, T. (2016). Platform Cooperativism: Challenging the Corporate Sharing Economy. New York, NY: Rosa Luxemburg Stiftung. Retrieved from: http://rosaluxspba.org/wp-content/uploads/2016/06/scholz_platformcooperativism_2016.pdf.

Solove, D. J. (2006). A brief history of information privacy law. In: Matthews, K. J. (ed.), *Proshauer On Privacy: A Guide to Privacy and Data Security Law in the Information Age*, New York, NY: Practising Law Institute., Retrieved from: http://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2076&context=faculty_publications.

Sorensen, B. M. (2009). How to surf: Technologies at work in the societies of control. In: Poster, M., & Savat, D. (eds.), *Deleuze and New Technology*, 63–81. Edinburgh: Edinburgh University.

Stalder, F. (2010). Autonomy and control in the era of post-privacy. 14 June. Retrieved from: http://felix.openflows.com/node/143.

Sullivan, B. (2006). 'La difference' is stark in eu, us privacy laws. *NBC News*, Oct. 19. Retrieved from: http://www.nbcnews.com/id/15221111/ns/technology_and_science-privacy_lost/t/la-difference-stark-eu-us-privacy-laws/#.V8b5qZMrLVo.

Szekely, I. (2014). The right to be forgotten and the new archival paradigm. In: Ghezzi, A., Pereira, S. G., & Vesnic-Alujevic, L. (eds.), *The Ethics of Memory in a Digital Age: Interrogating the Right to be Forgotten*, 28–49. London: Palgrave Macmillian.

Terranova, T. (2004). *Network Culture: Politics for the Information Age*. London: Pluto Press.

United States Department of Justice. (2015a). Privacy act of 1974. Retrieved from: https://www.justice.gov/opcl/privacy-act-1974.

United States Department of Justice. (2015b). Electronic communications privacy act of 1986. Retrieved from: https://www.justice.gov/jmd/electronic-communications-privacy-act-1986-pl-99-508.

Warren. S. D., & **Brandeis, L. D.** (1890). The right to privacy. *Harvard Law Review*, 4(5). DOI: https://doi.org/10.2307/1321160

Williams, R. W. (2005). Politics and self in the age of digital re(pro)ducibility. *Fast Capitalism*, 1(1). Retrieved from: https://www.uta.edu/huma/agger/fastcapitalism/1_1/williams.html.

How to cite this article: Weinberg, L. (2017). Rethinking Privacy: A Feminist Approach to Privacy Rights after Snowden. *Westminster Papers in Communication and Culture,* 12(3), 5–20, DOI: https://doi.org/10.16997/wpcc.258

Submitted: 30 January 2017 **Accepted:** 04 September 2017 **Published:** 31 October 2017

]u[*Westminster Papers in Communication and Culture* is a peer-reviewed open access journal published by University of Westminster Press **OPEN ACCESS**