International Journal of Communication 11(2017), Feature 4757–4768 1932-8036/2017FEA0002

Race, Class, and Privacy: A Critical Historical Review

MATT REICHEL
Rutgers University, USA

This essay inspects the maldistribution of privacy rights across race and class divisions by engaging a social history of the development of these rights from their inception in American jurisprudence. In so doing, it engages a critical theoretical framework that commences by delineating the contours of media structure, and then investigates how this structure bears on discourses about privacy and surveillance. Rather than viewing intrusions of privacy rights as a perversion of an otherwise egalitarian rights construct, this approach sees privacy discourse as a coded form of a more fundamental discussion about where individuals fit in to prevailing social hierarchies. In so doing, this essay shows how privacy and property rights have an intertwined history, through which an antagonism develops in capitalist society's attempt to balance property rights, social equity, and public trust. The resulting discourse on privacy is, then, reflective of this antagonism.

Keywords: privacy and media, privacy policy, social media and privacy, race and privacy, class and privacy, race class and privacy

Recent revelations of mass surveillance on the part of state investigative agencies and corporate entities have sparked renewed discourse concerning privacy rights, and the balancing thereof with security concerns in a digitized and networked world. The 2013 Snowden disclosures of dragnet surveillance by the National Security Agency (NSA), in particular, provoked widespread public outrage about privacy violations. In response, major technology companies have bowed to public pressure by increasingly encrypting user data on their networks and in their devices. However, many observers have noted that these protections have been implemented at an uneven pace across sociological categories such as race and class. Among others, the principal technologist at the ACLU, Chris Soghoian, remarked, "The phone used by the rich is encrypted by default and cannot be surveilled, and the phone used by most people in the global south and the poor and disadvantaged can be surveilled" (Simonite, 2015, para. 2). This gulf is largely a function of the fact that the more expensive iPhones come encrypted, whereas the vast majority of more affordable alternatives do not. Recent data from *The Wall Street Journal* show that 95% of iPhones in use are encrypted, compared with 2% of Android phones (Nicas, 2016).

This gap illustrates the fact that the right to privacy does not operate in its idealized form of equal protection for all members of society. This is a point that few would contest. However, the purpose of this article is not to argue that the prevailing model is broken, but rather that it is working as designed. The core objective of this essay is to demonstrate that an intrinsic connection exists between the

maldistribution of privacy rights and the broader social hierarchies that they reflect. For this reason, I find it more instructive to turn the traditional approach to privacy on its head, by seeing the discourse on the issue itself as reflective of more fundamental social divisions rather than seeing these divisions as a perversion of an otherwise egalitarian rights discourse. In this view, the fact that most Americans use vulnerable cell phones is reflective of privacy policy oriented toward protecting certain people, usually "good, law-abiding citizens," rather than trying to imagine a universal solution to the problem of mass surveillance. In other words, this thesis holds that political deliberation about privacy is, in fact, a coded conversation about the location of certain members of society in a social hierarchy, and that the unequal distribution of privacy rights effectively reifies this overarching hierarchy.

This thesis is divided into five sections. First, I will review some of the conventional literature on privacy, most of which focuses on legal and ethical concerns related to emerging privacy threats in the digital age. Second, I will pivot to the critical literature by developing a theoretical framework rooted in analyses of the impact of social structure on technological practice and of how this relates to privacy concerns. In the next two sections, I will look more closely at how these privacy concerns bear on class and race, respectively. Last, in the conclusion I will synthesize the foregoing analysis while making recommendations for activists concerned about the asymmetrical distribution of privacy rights across sociological categories.

The Dominant View on Privacy

A brief encapsulation of the dominant literature on privacy is in order before turning to the critical intervention that this article embraces. Much of this work occurs in the realm of law and ethics, and orients on discussions of the relationship between privacy and other fundamental goods and values (Moor, 2004; Solove, 2004; Spinello, 2015; Tavani & Moor, 2004). It is noteworthy that the dominant view, like its critical counterpart, generally sees privacy as being a derivation of something else, be it "security" (Moor, 2004; Tavani & Moor, 2004), "intimacy" (Fried, 1984; Nissenbaum, 2004), or "control" (Fried, 1984; Solove, 2004). Likewise, the right to privacy is not explicitly listed in the U.S. Constitution, but was rather found in the "penumbra" of the first and fifth amendments by the Supreme Court in *Griswold v. Connecticut*, as something that must be guarded to protect more basic rights (Moor, 2004; Osucha, 2009). In other words, privacy is widely seen as a necessary precondition for the realization of something more fundamental: a set of circumstances under which individual autonomy is made possible, so that other demands for human dignity can be made (Spinello, 2015). In this formulation, it is an "instrumental" rather than an "intrinsic" good: one that "is always desired for the sake of some other good, that is, as an instrumental means to some further end such as health or friendship" (Spinello, 2015, p. 303).

In other tracts, privacy is regarded as being a code word for another right or good, rather than as a conduit for the realization thereof. For example, Moor (2004) argues that it is an "expression of the value of security" (p. 411) in a highly complex and tech-laden society. He sees the strict intrinsic/instrumental dichotomy as problematic, because he views privacy as intrinsic to the value of security but instrumental to other core values, such as "life, happiness, freedom, knowledge, ability and resources" (p. 410). Meanwhile, Solove (2004) posits that privacy in the digital age is an expression of "control" over one's "digital dossier," that is, the wealth of data amassed about any individual, including

government records, consumer preferences, and spending habits. Along these lines, Fried (1984) holds that "privacy is not simply an absence of information about us in the minds of others, rather it is the control we have over information about ourselves" (p. 209). However, Tavani and Moor (2004) counter that control is, in fact, a justification for privacy, as well as an aspect of the management of privacy, rather than something that inheres in privacy itself. In this vein, they see control and privacy as "complementary notions that reinforce each other" (p. 440). A greater degree of control over data related to oneself is a principal justification for privacy, while the affordance of greater privacy, in turn, permits individuals to manage, or control, the level of publicity that they subject themselves to.

The proposed solutions to the threat to privacy posed by digital communication technologies vary, but tend to center on the need to create space for privacy to flourish within certain conditions. Tavani and Moor (2004) advocate for the creation of "zones of privacy" governed by the principle of "restricted access" and managed according to the maxim of "limited control." This approach is a recognition of the limitation of control theories of privacy in an information age where complete control is impractical. Such theories hold that privacy policy should be focused on guaranteeing that "only the right people have access to relevant information at the right time" (Moor, 2004, p. 414). In this view, the objective is to maximize the amount of control individuals possess over their data, rather than to see complete control as the essence of what privacy is.

Meanwhile, Nissenbaum (2004) advocates using the guiding principle of "contextual integrity" with regard to privacy policy, recognizing that it is not only the content but also the context in which information is shared that is vital in determining whether a harm has been committed. She holds that privacy protections should emphasize placing restrictions on the capacity of tech companies to sell user data to secondary entities beyond what is reasonable for advertising purposes. Solove (2004) concurs that more must be done to allow individuals to make informed choices about the use of their digital information. He writes of the importance of recognizing "architectural" aspects to privacy, so as not to be reliant on individual grievances raised through the legal process. Instead, he argues that the structure of relationships between individuals and businesses and government should be regulated in a way that will prevent the breaches of privacy that emerge as "consequences" of current structure.

Solove's (2004) emphasis on structure provides an important bridge to the discussion of the critical literature on privacy that follows. The difference between conventional and critical approaches, after all, turns on the stress placed on social structure as conditioning human relations. However, Solove's structure is one composed of atomized individuals interacting with governments and businesses governed by a set of laws, rather than a social structure composed of myriad groups ordered into a contradictory and conflict-ridden totality. Hence, he believes it to be a trivial thing to compose a new structure that permits greater individual participation in the collection and use of their information. A critical approach, meanwhile, recognizes that new structures are not simply engineered, but rather emerge through a prolonged process of struggle among social groups over the form and function of society (Fuchs, 2010; Sewell, 2005).

The critical approach does not generally dispute the importance of privacy for notions of autonomy, control, security, and intimacy, nor does it necessarily take issue with formulating legalistic

responses to certain violations of privacy. It does, however, contend that the conventional approach misses the fact that privacy invasions naturally follow existing sociological divisions, owing to the impact of social structure on technological practice (Fuchs, 2010). This is to say that the "architecture" in which individuals interact with technology is not neutral: It is, instead, reflective of extant societal prejudices and power asymmetries. Moreover, the legalistic approach is simply not adequate to address these structural biases, even if it can correct some of the most egregious wrongs.

The race and class-based divide on smartphone encryption is a case in point. This fissure developed around existing structures, wherein certain members of society are in possession of the wealth and technological proficiency requisite to keep their digital footprint relatively secure, and others are simply looking for the cheapest phone available. Android-based phones have filled the demand for the latter, despite some recent moves to guarantee a greater level of protection for users in recent years. Because the software developer, Google, does not also manufacture the hardware, it has not generally been able to guarantee encryption across all devices (Cipriani, 2016). Although some of the newer, higher-end Android phones come with encryption enabled, the vast majority of older and entry-level phones still do not (Cipriani, 2016), so that the cross-platform encryption divide is effectively reinforced within platforms.

In this sense, privacy often takes on the characteristics of a commodity. As will be discussed in the following sections, the amount of privacy one is able to attain is related to one's wealth and overall position in society: It has simply never been equitably distributed across the population (Bauman, 2013; Bigo, 2006; Giroux, 2015). Put simply, those with a larger private realm have access to more privacy than those in possession of limited or no private property. In other words, privacy might well be intrinsic to one's security, and instrumental to happiness and freedom, as Tavani and Moor (2004) contend, but it is also intrinsic to wealth, and, by extension, instrumental to one's social status.

Theoretical Framework: Media Structure and the Privacy/Surveillance Duality

This critical intervention recognizes that it is best to chart the outline of the forest before getting lost in the trees—that is, to appreciate that broad social inequalities exist prior to individual manifestations thereof. As such, this section will commence with a delineation of social structure before looking at how it bears on the race and class dynamics in the context of contemporary American society.

The structure embraced here is not a static one, but rather one that sees the social world as an ever-evolving "cultural construct" (Sewell, 2005, pp. 16–17). Sewell holds that social science investigations should read like a historical narrative in which individuals interact with structures and their embedded schemas and logics in a dynamic world. In this case, we develop an understanding of the social function of "privacy" in the current era through an examination of its historical development through prior technological forms, before then glimpsing current debates within this established context.

Sewell's notion borrows from Giddens' (1984) "duality of structure," through which Giddens overcomes the subject/object dichotomy by seeing the two elements as mutually constitutive of structure. On the implications of this formulation for the study of the media, Fuchs (2010) relates:

> Media structures and media practices are dialectically connected and produce each other so that the media system is a dynamic system that is reproduced through a dialectic of media subjects (human actors who engage in media production and reception) and media objects (media structures). (p. 174)

That being so, the media landscape is constitutive of the various practices employed by users who are, in turn, a product of that landscape.

In this formulation, the privacy rights discourse emerges from media practices that introduce a fundamental contradiction within capitalism by threatening to overexpose it. Fuchs (2012) argues that a core function of privacy in liberal society is to obscure wealth, so that social inequalities are not in plain view. Because the legitimacy of the prevailing social order rests, in large part, on the conceit that most people are starting from relatively equal footing, it is necessary to conceal the fact that this is not, in fact, the case. As evidence of the efficacy of this mechanism in contemporary times, Norton and Ariely (2011) conducted a nationwide survey to inspect Americans' view of wealth inequality and found that "respondents vastly underestimated the actual level of wealth inequality in the United States, believing that the wealthiest quintile held about 59% of the wealth when the actual number is closer to 84%" (p. 10). The view most people have of economic structure is highly divergent from reality, which suggests that privacy rights are working according to Fuchs' model.

It is also important to consider what is exposed, rather than hidden, in determining the contours of privacy rights and how they navigate systemic contradictions. If the legitimacy of capitalism rests on concealing wealth asymmetries from view, it also requires acquisition of information on strangers in order to be able to conduct business. In valuing the privacy of wealth holdings simultaneously with the ability of individuals to engage in free exchange, capitalism practically requires routine surveillance. Fuchs (2012) notes:

> The establishment of trust, socio-economic difference, and corporate interests are three qualities of modernity that necessitate surveillance. Therefore, modernity on the one hand advances the ideal of a right to privacy, but at the same time it must continuously advance surveillance that threatens to undermine privacy rights. An antagonism between privacy ideals and surveillance is therefore constitutive for capitalism. (p. 46)

In sum, privacy and surveillance represent two sides of an antagonism that inheres in capitalist society's attempt to balance property rights, social equity, and public trust. Meanwhile, media structure is constitutive of this antagonism, whereas media discourses both reify and contest the embedded power asymmetries. Within these discourses, privacy advocacy comes to serve principally as a means by which property rights are protected and public trust is guaranteed through the obscuration of underlying social inequities (Fuchs, 2012; Osucha, 2009).

To glimpse this interplay between privacy and surveillance in practice, it is instructive to look at the history of these rights in American jurisprudence. The notion of a "right to privacy" was first introduced by Samuel Warren and Louis Brandeis in the *Harvard Law Review* in 1890; it expressed

concerns over the potential "invasion" of the private realm by "instantaneous photographs and newspaper enterprise" (p. 195) and the threat this posed to "man's house as his castle" (p. 220). Meanwhile, the Supreme Court, in *Griswold v. Connecticut*, found privacy rights as residing in the "penumbra" of the first and fifth amendments (Osucha, 2009). In this view, privacy guarantees inhere in free speech rights because they cover the obverse condition. If one's right to assert oneself publicly is protected, then surely, so is the right to retreat to the comfort of home. Privacy's connection to property is intrinsic.

Class, Capitalism and Privacy

What follows is a brief social history of how privacy and property rights have developed within the context of 20th-century American history, and how this informs the development of current media structure and its constituent practices. In engaging the theoretical framework developed in the prior section, I will treat privacy and surveillance as constituting a duality employed to mediate the process of distributing the rewards of the capitalist economy. Such is essentially the argument of McChesney and Foster (2014) in their recounting of the history of "surveillance capitalism"—a structure that they contend was built around the two "surplus absorption mechanisms" of a Madison Avenue–based sales economy, on the one hand, and the warfare state, on the other. Later, in response to the economic crisis of the 1970s, a third pillar of finance was appended, with all three contributing separately to the ongoing "communication revolution," through which the privacy and security of various subjects in society is determined.

McChesney and Foster's (2014) time line commences in the postwar years, when civilian and military technological development were brought into alignment in what they call "military Keynesianism." Ultimately, this formulation faced a significant contradiction in the form of resistance to the warfare state. In response, political elites fought for the expansion of propaganda and surveillance capacities. The necessary communication technologies were brought over from the corporate world, where the surveillance capacities were used to track consumer behavior. Gradually, these technologies would be incorporated into military systems through the creation of the Advanced Research projects Agency (ARPA) and through the implementation of ARPANet, the precursor to the Internet, which, at the time, was used for the transmission of information gleaned from the surveillance of antiwar activists and other dissidents. Despite public outcry, surveillance activity would expand shortly thereafter under the NSA's ECHELON and MINARET programs (McChesney & Foster, 2014).

Meanwhile, the U.S. economy entered a period of stagnation on the heels of the Vietnam War that precipitated the neoliberal turn to finance, which accelerated under the Reagan administration. Significantly, this "financialization" occurred alongside rapidly expanding networking and computing technologies, which permitted surveillance capitalism to expand, so that every aspect of one's life could be converted into data and incorporated into profit-driving algorithms. Parenti (2003) described this process: "The records produced by credit cards, bankcards, discount cards, Internet accounts, online shopping, travel receipts and health insurance all map our lives by creating digital files in corporate databases" (pp. 91–92, 96).

This history depicts a close relationship between military and corporate power in their employment of communication technologies for surveillance purposes. The need to monitor citizens

mirrors the impulsion to do the same to consumers, insofar as both seek to exert control over an external population to secure a privileged core. Moreover, this intertwining of capitalism and surveillance is not unique to the United States, but emerges out of the fundamental contradictions of liberal societies discussed in the previous section. For wealth to be generated, information must be gleaned through practices of surveillance, at the same time that society pretends to guarantee universal privacy rights, which are, in practice, generally in place to obscure the maldistribution of wealth.

These contradictions have arguably risen to the fore in the age of social media, wherein companies like Facebook rely on user-generated data to sell to advertisers in what is essentially an intensified version of Smythe's (1981/2006) notion of the "audience commodity" (Fuchs, 2012). The difference is that the social media audience willfully gives up its privacy rights. Users gain the capacity to share with a network of friends and associates in exchange for having their privacy invaded for the benefit of the profit of social media companies, which, McChesney (2013) reports, are now among some of the largest in the global economy.

It is also worth noting that when the audience is treated as a commodity in this way, so is privacy. Far from being a right spread across the totality of society, it takes a "possessive individualistic" form wherein individuals can dispense with it as they please (Sevignani, 2013). Other scholars, such as Albrechtslund (2013), contest this notion of a commodified form of rights, arguing that a new model is needed that acknowledges the act of sharing as being separate from commercial exchange. However, this criticism fails to appreciate the historic intertwining of privacy and property rights as discussed in this article. If one accepts that privacy exists to provide cover for one's wealth, then relinquishing privacy is the equivalent of exposing one's property to the public in exchange for gaining social status. As part of this process, the line between the public and private domains gets blurred in the digital age (Papacharissi, 2010). For that reason, what is needed more than a model of how people share is a new model for how the public–private binary gets renegotiated.

With the advent of social media, the private realm now serves increasingly as the location of social engagement, through which status and economic privilege are gradated. This happens on two fronts. On the one hand, users gain social status through the attention and visibility they attain in building a social media following. As Marwick (2013) notes in her ethnography on the Silicon Valley tech scene, the notion of status being conferred through visibility is a cultural trait of the region that has effectively been implanted into social media logics. Meanwhile, on the other hand, commercial interests are ever engaged in classification of its consumer base in what Gandy (1996) terms the "panoptic sort," wherein consideration is made of "all information about individual status and behavior to be potentially useful in the production of intelligence about a person's economic value" (p. 133).

In either case, one cannot afford to remain private, for one must be present if one is to secure the benefits of these sorting mechanisms. The result has been what some scholars characterize as a flight from privacy. Visibility is sought rather than privacy, so that now the history of surveillance capacities has come full circle. Technologies that were originally deployed to track consumer behavior are now used by willing subjects fearing the prospect of being left out (Giroux, 2015). However, one's desire to participate

has not proven adequate to guarantee one's inclusion, because the willing participation of status-seekers and consumers are not the mechanisms determining the contours of social hierarchies.

Race, Ethnicity, and Privacy

A more exclusionary form of surveillance also exists, largely for what Wacquant (2007) describes as the "outcasts" of contemporary society. In the extreme, this phenomenon takes the form of the migrant—those with no privacy to exchange for gains in social prestige. They lack grounding, existing in a state of what Agier (2011) calls "liminal drift," thoroughly cut off from the idealized "castle" of Warren and Brandeis (1890).

In short, discourse on privacy not only mediates degree of value in a capitalist society but also determines whether one is permitted meaningful value at all in a racialized society. With this, the discussion turns from the classification and assessment of commodified privacy actuated by the "panoptic sort" to the realm of racial and ethnic exclusion through what Bigo (2006) calls the "ban-opticon." He describes a threefold process by which certain segments of the population are banned. First, there is the declaration of permanent states of emergency through which "exceptional" power is claimed. Second, certain groups are routinely profiled as warranting suspicion and extra scrutiny, as evinced by the heightened level of surveillance of Muslim Americans in the United States since 9/11. Last, the ban-opticon legitimizes itself through the employment of propaganda that convinces sufficient portions of the population of the merits of the dominant ethos of that society.

As such, the privileged groups are convinced of the virtue of the social order they benefit from, while being told that any limitations on the "rights" of certain people is justified on security grounds. This arrangement is further concretized through a continued framing of privacy concerns in the language of "rights," as if government surveillance were a harm in need of remediation rather than a process by which structural hierarchies are determined. An overreliance on rights language risks treating all members of society uniformly, even though the very nature of surveillance practice is to differentiate across sociological category.

Of particular concern to this project is the danger that this overreliance could lead to an embrace by activists of "targeted surveillance" instead of mass surveillance—that is, eschewing the panopticon for the ban-opticon. Gürses et al. (2016) see this shift as being marked in the transition to economic arguments concerning surveillance, wherein privacy advocates have emphasized the "effectiveness" of various approaches to security, with mass surveillance seen as being wasteful and unnecessary. These approaches view encryption as a way to compel government agencies to revert to targeted surveillance because of cost concerns, which the authors believe will largely translate into a focus on Muslim-Americans, given revelations about NSA and FBI targeting of this community.

In other words, *targeted surveillance* serves as coded language for the prevailing system in which racial and ethnic exclusivity is mediated by the privacy/surveillance debate. Giroux (2015) notes that "people of color, especially poor dissenting blacks" (p. 157), have never had a reasonable expectation of privacy in the United States. He continues, "The right to privacy was violated in the historical reality of

slavery, the state terrorism enacted under deep surveillance programs such as COINTELPRO, and in the current wave of mass incarcerations" (p. 157). Another recent example includes New York City's use of "stop and frisk" policing, which civil rights advocates have widely denounced for its targeting of people of color.

This bifurcation between protected and surveilled groups emerged in the early discourses around privacy in this country. Osucha (2009) charted this history from its inception in Warren and Brandeis's (1890) idealized castle onward. She notes that public outrage swirled around details of *Roberson v. Rochester Folding Box Co.*, in which a young, White woman claimed that her visage had been appropriated for use on boxes of flour mix. In contradistinction, similar appropriation of overtly racist southern black archetypes, including Aunt Jemima, were viewed as natural. Osucha sums up:

> That, in the same historical moment, the literal commodification of one woman—African American, elderly, working class—would be enthusiastically embraced by American consumers, while another—white, young, bourgeois, woman's rather tenuous, purely symbolic claim of commodification was met with proportionate horror and condemnation helps highlight . . . the specific racial, gendered, and class contours of the injuries claimed by Abigail Roberson and of the legal doctrine that this seminal lawsuit engendered. (p. 87)

She holds that this is a demonstration of the fact that the private/public duality corresponds, more or less, to the delineation between whiteness and blackness in the United States, noting that "to be subject to media publicity is to be, in effect, racialized" (p. 73).

Thus, there are two effects of the mediation of race and ethnicity by the privacy discourse. One effect is to ban the racial/ethnic other from the privileges of commodified privacy, while the other effect is to situate a stereotypical form of this other in the realm of the public. In this sense, the proverbial castle delineates the insides from the outsides of society: a privileged Whiteness that resides inside, and an outside that is ever exposed, both subjected to heightened surveillance and reduced to racist tropes (Osucha, 2009). Moreover, this function tends to work in a purely dualistic fashion, rather than in the gradated manner of the panoptic sort. Put simply, subjects are either afforded some access to the castle, however limited it may be, or they are effectively banned.

The current debates concerning encryption and surveillance demonstrate this dynamic rather neatly. The former has been widely viewed as the solution to the problem of overzealous employment of the latter by intelligence agencies, but minimal effort has been made to ensure protection across race, ethnic, and class lines. Instead, encryption has merely amplified existing sociological divisions. Meanwhile, the divergent public responses to mass versus targeted surveillance have mirrored the previous reactions to appropriations of White versus Black likenesses in the case of Roberson and Aunt Jemima. When the privacy of the privileged subject is violated, it provokes collective outrage, whereas surveillance of the other is tolerated and even desired. The result is marked historical continuity in the race and ethnic function of the privacy discourse in American society, even though some of the more extreme and violent expressions of racism are no longer collectively tolerated. Liberal society has become more tolerant, to be

sure, but the underlying racialized structure still exists, and it manifests in this realm by determining who possesses privacy and who possesses the watchful gaze of the state and its privileged population.

Conclusion

This article holds that there is significant divergence between the dominant view of privacy and how privacy actually functions in capitalist society, where discourses on privacy serve to delineate the bounds of access and privilege. Within a social structure marked by inequities across race and class, the distribution of privacy rights will follow suit, effectively defending the wealth of the few while banishing the most marginalized and vulnerable to an existence outside of the protections of these rights. When one embraces privacy as a virtue, one also embraces the security that inheres in it: a desire to be safely tucked away inside, protected from an undesirable other.

This is not to suggest that NSA snooping is not a legitimate concern, but rather to suggest that the impulse of governments to snoop is rooted in privacy demands. The moment one expresses a desire to be secure at home, one must define an exteriority from which to be secured against. Adopting the privacy rhetoric sets off a vicious circle. If encryption were offered across all platforms, intelligence agents would likely adopt new ways of infiltrating targeted populations' devices while inventing new threats to the security of the privileged population.

Rather than using this rights construct that has these sorting and banning functions embedded, progressive activists should orient their energies toward criticizing the impulsion to divide populations by the degree to which they fit into an idealized core. Instead of drawing lines dividing segments of the population, as privacy language demands, progressives should advance a politics of radical inclusivity rooted in a robust and dynamic public sphere. The desire should not be hiding away in a castle, but be manifest in radical social engagement, which means an embrace of a common fraternity across race, class, nation, and ethnicity. Meanwhile, the harm promulgated by government spying should be viewed as infringing upon one's dignity and not one's privacy. This is especially the case when whole groups of people have historically never had any reasonable expectation of privacy to defend, and others have so little it is hardly worth noting. Instead, a progressive worldview ought to envision equal dignity across all people: a dignity rooted in the ability to move, think, and express oneself without undue interference.

References

Agier, M. (2011). *Le couloir des exiles. Etre etranger dans un monde commun* [The corridor of exiles: Being foreign in a common world]. Marseille, France: Editions du Croquant.

Albrechtslund, A. (2013). New media and changing perceptions of surveillance. In J. Hartley, J. Burgess, & A. Bruns (Eds.), *New media dynamics* (pp. 311–321). Hoboken, NJ: Blackwell.

Bauman, Z. (2013). *Liquid surveillance*. Cambridge, UK: Polity Press.

Bigo. (2006). Globalized (in)security: The field and the ban-opticon. In N. Sakai & J. Solomon (Eds.), *Traces 4: Translation, biopolitics, colonial difference* (pp. 5–49). Hong Kong: Hong Kong University Press.

Cipriani, J. (2016). What you need to know about encryption on your phone. *CNET*. Retrieved from https://www.cnet.com/news/iphone-android-encryption-fbi/

Fried, C. (1984). Privacy: A moral analysis. In F. D. Schoeman (Ed.), *Philosophical dimensions of privacy: An anthology* (pp. 203–223). Cambridge, UK: Cambridge University Press.

Fuchs, C. (2010). Alternative media as critical media. *European Journal of Social Theory, 13*(2), 173–192.

Fuchs, C. (2012). Critique of the political economy of Web 2.0 surveillance. In C. Fuchs, K. Boersma, A. Albrechtslund, & M. Sandoval (Eds.), *Internet and surveillance: The challenges of Web 2.0 and social media* (pp. 31–70). New York, NY: Routledge.

Gandy, O. (1996). Coming to terms with the pan-optic sort. In D. Lyon & E. Zureik (Eds.), *Computers, surveillance, and privacy* (pp. 132–155*)*. Minneapolis. MN: University of Minnesota Press.

Giddens, A. (1984). *The constitution of society: Outline of the theory of structuration.* Berkeley, CA: University of California Press.

Giroux, H. (2015). Selfie culture in the age of corporate and state surveillance. *Third Text*, *29*(3), 155–164.

Gürses, S., Kundani, A., & Van Hoboken, J. (2016). Crypto and empire: the contradictions of counter-surveillance advocacy. *Media, Culture, and Society,* 38(4), 576-590.

Griswold v. Connecticut, 381 U.S. 479 (1965).

Marwick, A. (2013). *Social status*. New Haven, CT: Yale University Press.

McChesney, R. W. (2013). *Digital disconnect: How capitalism is turning the Internet against democracy*. New York, NY: New Press.

McChesney, R. W., & Foster, J. (2014). Surveillance capitalism. *Monthly Review*, *66*(3), 1–31.

Moor, J. (2004). Toward a theory of privacy for the Information Age. In R. Spinello & H. Tavani (Eds.), *Reading in cyberethics* (2nd ed., pp. 407–417). Boston, MA: Jones and Bartlett Publishers.

Nicas, J. (2016, March 14). Google faces challenges in encrypting Android phones. *The Wall Street Journal.* Retrieved from http://www.wsj.com/articles/google-faces-challenges-in-encrypting-android-phones-1457999906

Nissenbaum, H. (2004). Toward an approach to privacy in public: Challenges of information technology. In R. Spinello & H. Tavani (Eds.), *Reading in cyberethics* (2nd ed., pp. 450–461). Boston, MA: Jones and Bartlett Publishers.

Norton, M., & Ariely, D. (2011). Building a better America—One wealth quintile at a time. *Psychological Science, 6*(1), 9–12.

Osucha, E. (2009). The whiteness of privacy: Race, media, law. *Camera Obscura*, *24*(1), 67–107.

Papacharissi, Z. (2010). *A private sphere: Democracy in a digital age.* Malden, MA: Polity Press.

Parenti, C. (2003). *The soft cage: Surveillance in America: From slavery to the war on terror*. New York, NY: Basic Books.

Roberson v Rochester Folding Box Co., 171 N.Y. 538, 64 N.E. 442 (1902).

Sevignani, S. (2013). The commodification of privacy on the Internet. *Science and Public Policy, 40*, 733–739.

Sewell, W. (2005). *Logics of history*. Chicago, IL: University of Chicago Press.

Simonite, T. (2015, November 3). Why Google trailing Apple on encryption support is a human rights issue. *MIT Technology Review.* Retrieved from https://www.technologyreview.com/s/543161/why-google-trailing-apple-on-encryption-support-is-a-human-rights-issue/

Smythe, D. (2006). On the audience commodity and its work. In M. G. Durham & D. Kellner (Eds.), *Media and cultural studies* (pp. 230–256). Malden, MA: Blackwell. (Original work published 1981)

Solove, D. (2004). *The digital person: Technology and privacy in the Information Age*. New York, NY: New York University Press.

Spinello, R. (2015). The right to privacy in the age of digital technology. In S. Zeadally & M. Badra (Eds.), *Privacy in a digital, networked world: Technologies, implications and solutions* (pp. 291–312). New York, NY: Springer Publishing.

Tavani, H., & Moor, J. (2004). Privacy protection, control of information, and privacy-enhancing technologies. In R. Spinello & H. Tavani (Eds.), *Reading in cyberethics* (2nd ed., pp. 436–449). Boston, MA: Jones and Bartlett Publishers.

Wacquant L. (2007). *Urban outcasts: A comparative sociology of advanced marginality*. Cambridge, UK: Polity.

Warren, S., & Brandies, L. (1890). The right to privacy. *Harvard Law Review, 4*, 193–220.